# Rekisterinpitäjän osoitusvelvollisuus

## Tietosuojaviranomaisen ennakko- ja jälkivalvonta konsernin näkökulmasta

**Joona Linner**

**Rekisterinpitäjän osoitusvelvollisuus**

**Pro gradu -tutkielma**

**Hallinto-oikeus**

**Kevät 2020**

**Lapin yliopisto**

**Tekijä** Joona Linner

**Työn nimi** Rekisterinpitäjän osoitusvelvollisuus – Tietosuojaviranomaisen ennakko- ja jälkivalvonta konsernin näkökulmasta

**Tutkinto** Oikeustieteiden maisteri

**Koulutusohjelma** Oikeustiede

**Työn ohjaaja(t)** Kirsi Kuusikko

**Hyväksymisvuosi** 2020 **Sivumäärä** XXVIII + 109 **Kieli** Suomi

**Tiivistelmä**

Tämä oikeusdogmaattinen tutkielma käsittelee eurooppalaista tietosuojalainsäädäntöä, joka on lainsäädäntöalueena pitkälti harmonisoitu jäsenvaltiossa. Tulen ottamaan kantaa siihen, mitä yhtäläisyyksiä ja eroavaisuuksia edeltäneen ja nykyisen tietosuojalainsäädännön välillä on, sillä erityisesti yhtäläisyyksien osalta voidaan huomioida aikaisempi oikeuskäytäntö vähintäänkin analogisesti. Tutkielmassa arvioidaan myös lainsäädännöllisten muutosten tarpeellisuutta nykyisen verkko- tai pikemminkin ubiikkiyhteiskunnan aikakaudella. Aiheeseen johdatuksena voidaan todeta, että globalisaatio sekä työvoiman, pääoman, tavaroiden ja palveluiden vapaa liikkuvuus unionin sekä Euroopan talousalueella ovat synnyttäneet tarpeen säännellä henkilötietojen käsittelyä yhä enenevässä määrin harmonisoidusti subsidiariteettiperiaatteeseen nojautuen. Aikaisemmin voimassa olleen direktiivin 95/46/EC (*Henkilötietodirektiivi*) aikakaudella ongelmaksi nousi se, että käytännössä unionin alueella oli 28 erilaista tietosuojalakia, joita monikansallisten yhtiöiden oli hankala noudattaa yhtäaikaisesti. Näin ollen päätettiin säätää yleinen tietosuoja-asetus (EU) 679/2016 (GDPR), jonka avulla sovellettavaa tietosuojalainsäädäntöä saatiin harmonisoitua kattavammin. GDPR tulee sovellettavaksi myös tilanteissa, joissa henkilötietoja siirretään EU/ETA:n ulkopuolelle.

Unionin integraatiokehityksen tuotteena syntyvän lainsäädännön harmonisoitumisen henkilötietojen suojan alueella, on nähty lisäävän yksilöiden mahdollisuuksia panna täytäntöön heille kuuluvia yksityisyyteen sekä henkilötietojen suojaan liittyviä oikeuksiaan. GDPR:ään perustuen Suomen aikaisempi tietosuojan yleislaki, henkilötietolaki, kumottiin uudella tietosuojalailla, jonka puitteissa on käytetty tietosuoja-asetuksen jäsenvaltioille suomaa liikkumavaraa. Tutkielman päätavoitteena on kuitenkin arvioida nimenomaisesti tietosuoja-asetuksen mukaisen osoitusvelvollisuuden sisältämiä toimintavelvoitteita konsernin näkökulmasta. Tällöin tutkimuskysymykseksi asettuu se, miten osoitusvelvollisuus on täytettävissä ja miten tämä on osoitettavissa tietosuojaviranomaiselle tämän suorittamassa ennakko- ja jälkivalvonnassa. Osoitusvelvollisuuden täyttäminen käytännön tasolla on jaettu tutkielmassa tilanteisiin, joissa on kyse rekisterinpitäjän sisäisestä käsittelytoiminnasta sekä tilanteisiin, joissa on kyse rekisterinpitäjän ulkoistamasta sen lukuun tapahtuvasta tietojenkäsittelytoiminnasta. Koska jokainen yhtiö käsittelee vähintäänkin työntekijöidensä henkilötietoja työoikeudelliseen lainsäädäntöön perustuen, ei yhteisöt voi välttyä täysin GDPR:n soveltamiselta.

On syytä huomata, että tietosuojassa on kyse perus- ja ihmisoikeuksien suojaamisesta, mistä säädetään Suomen perustuslain 10.1 §:n ohella Euroopan perusoikeuskirjassa ja joka on johdettavissa myös Euroopan ihmisoikeussopimuksesta sekä useista YK:n valtiosopimuksista. Euroopan tietosuojauudistuksen myötä oikeutta henkilötietojen suojaan ylläpidetään entistä tehokkaammin keinoin. Tästä esimerkkinä, ja suhteessa henkilötietodirektiiviin tapahtuneena muutoksena, voidaan mainita hallinnolliset sakot, joita voidaan nykyisin määrätä organisaatiolle, joka toimii tietosuojalainsäädännön vastaisesti. Toisena eroavaisuutena on tämän tutkielman aiheena oleva osoitusvelvollisuus, josta säädetään tietosuoja-asetuksen 5(2) artiklassa ja jonka perusteella rekisterinpitäjä on vastuussa siitä, että tämän käsittelytoiminnassa noudatetaan kaikkia GDPR:ssä määriteltyjä tietosuojaperiaatteita ja lisäksi rekisterinpitäjän on kyettävä osoittamaan myös jälkikäteen noudattavansa näitä periaatteita.

**Avainsanat** Tietosuoja, rekisterinpitäjä, osoitusvelvollisuus

University of Lapland

**Author** Joona Linner

**Title of thesis** The Accountability of the Data Controller – Pre-control and Ex-post Administrative Control by the Data Protection Authority from the Perspective of Group of Undertakings

**Degree** Master of Laws

**Degree programme** Degree programme in law

**Thesis advisor(s)** Kirsi Kuusikko

**Year of approval** 2020 **Number of pages** XXVIII + 109 **Language** Finnish

## Abstract

This thesis discusses with Finnish and European data protection law which is part of the Finnish law system nowadays. In particular, I will address the issue from the point of view of changes and similarities between previous and current applicable data protection law. In the thesis, the necessity of the current state of justice is also considered. As an introduction to the subject, globalization and the free movement of labor, goods, capital and services within the European Union have led to the need to regulate further the processing of personal data. Our previous national data protection legislation is based on Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data (the "Personal Data Directive"). However, the problem has been that the Directive has made it possible for Member States of the European Union (EU) to have 28 different regimes of data protection within the EU. As a mandatory instrument, the General Data Protection Regulation (EU) 679/2016 (GDPR) will further harmonize data protection legislation within the EU. The GDPR also regulate the obligations under which personal data may be transferred to third countries.

The harmonization of data protection practices is considered to give EU citizens greater confidence in the processing of their personal data. However, the GDPR does not charge to any great extent the general principles relating to the processing of personal data. As a change, the Finnish Personal Data Act has been replaced by a new law named as the Data Protection Act. The content of the new Data Protection Act must be compatible with the content of the General Data Protection Regulation and derogations from the Regulation may only be regulated to the extent that the Regulation allows within the leeway of that Regulation. It should also be emphasized that the General Data Protection Regulation applies to all companies, regardless of their size. Because every company processes personal data regardless of industry, due to labor law obligations, the requirements of the GDPR cannot be completely avoided. In practice, the processing of personal data of any customer or employee results in the application of the General Data Protection Regulation.

According to the GDPR, "the protection of individuals with regard to the processing of personal data is a fundamental right". It is also stated "everyone has the right to the protection of personal data concerning them". This is consistent with Section 10(1) of the Constitution of Finland (731/1999), which states "Everyone's private life, honour and the sanctity of the home are guaranteed. More detailed provisions on the protection of personal data are laid down by an Act." As mentioned above, the Constitution requires that there shall be more stringent legal provisions regulated on data protection.

Article 83 of the GDPR provides for administrative fines that can be imposed by the Data Protection Authority in event of a breach of the data protection obligations under the GDPR. These administrative sanctions act as deterrents in general to ensure that data controllers and processors are sufficiently serious and accurate in respecting the privacy obligations of individuals. The only different at the level of general principles of data protection law regulated by the GDPR is the so-called principle of the accountability of the data controller. It is stipulated in Article 5(2) of the GDPR, that requires the controller to demonstrate compliance with all principles relating to the processing of personal data under the Regulation and in particular, the controller is, in addition, responsible for complying with the requirements in accordance with those principles.

**Keywords** Data protection, controller, accountability

# SISÄLLYS

# LÄHTEET

## Kirjallisuus ja tieteelliset artikkelit

*Aarnio, Aulis*. Arvot lainkäytössä. Valtakunnan syyttäjänviraston julkaisusarja n:o 5: Arvot ja periaatteet. Valtakunnansyyttäjävirasto: Helsinki 2007, s. 15—27.

*Aarnio, Aulis*. Lainoppi. Encyclopaedia Iuridica Fennica 7, Oikeuden yleiset tieteet. Suomen lakimiesyhdistys, Helsinki 1999, s. 331—337.

*Aarnio, Aulis*. Oikeusvaltio. Toim. Aulis Aarnio ja Timo Uusitupa. Vantaa 2002.

*Adshead, Deborah*. Impact of EU-GDPR on Local Authorities in UK. Sheffield Hallam University 2016.

*Alapuranen, Leena – Heino, Anna-Maija – Salli, Minna – Koskinen, Seppo*. Henkilötietojen käsittely työelämässä. Edita Oyj: Helsinki 2005.

*Alén-Savikko, Anette*. Ennaltaehkäisy, hyvinvointipalvelut ja työntekijän tietojen hyödyntäminen – Katsaus tietosuojaan työterveydessä. Artikkeli on kirjoitettu osana Tekesin rahoittamaa Digital Health Revolution -projektia. Teoksessa Viestinnän muuttuva sääntely - Viestintäoikeuden vuosikirja 2016, toim. Päivi Korpisaari, Helsinki 2017, s. 94—111.

*Andersson, Jenna*. Organisaation tietoturva- ja tietosuojariskienhallinta sekä lainsäädännön vaatimukset. Referee-artikkeli, Edilex artikkelit, Edita Publishing Oy, 4/2018.

*Belinskij, Antti – Warsta, Matias – Ekroos, Ari – Määttä, Tapio*. Yhden lukuun periaate ympäristöllisissä ennakkovalvonta- ja suunnittelumenettelyissä: Väliraportti 15.1.2016, Itä-Suomen yliopisto ja Enlawin Consulting Oy 2016.

*Blume, Peter*. Controller and processor: Is there a risk of confusion. International Data Privacy Law, Volume 3, Issue 2, Oxford 2013, s. 140—145.

*Blume, Peter*. Privacy as a Theoretical and Practical Concept. International Review of Law. Computer Law & Technology. Volume 11, Issue 2, 1997, s. 193—202.

*Brownsword, Roger – Somsen, Han*. Law, Innovation and Technology: Before We Fast Forward – A Forum for Debate. Published online in ResearchGate 2009.

*Brouwer, Evelien*. Legality and Data Protection Law: The Forgotten Purpose Limitation. Teoksessa The Eclipse of the Legality Principle in the European Union. Toim. Leonard F.M. Besselink, Frans Pennings, Sacha Prechal, Alphen Van den Rijn. Kluwer Law International 2010, s. 273—294.

*Bygrave, Lee.* Data Protection Law: Approaching Its Rationale, Logic and Limits. Kluwer Law International, 2002.

*Calder, Alan*. EU GDPR & EU-US Privacy Shield – A Pocket Guide. IT Governance Publishing, UK, Cambridge 2016.

*Carey, Peter – Denham, Elizabeth*. Data Protection – A Practical Guide to UK and EU Law. (5. painos) Oxford University Press 2018.

*Craig, Paul – de Búrca, Gráinne*. EU Law – Text, Cases and Materials. (6. painos) Oxford University Press 2015.

*Determann, Lother*. Determann's Field Guide to Data Privacy Law – International Corporate Compliance. (3. painos) Edward Elgar Publishing, UK: Cheltenham, USA: MA, Northampton 2017.

*Ferretti, Federico*. Data Protection and the Legitimate Interest of Data Controller: Much ado about nothing or the winter of rights? Common Market Law Review, Volume 51, Issue 3, Kluwer Law International 2014, s. 843—868.

*McGeveran, Williams.* Privacy and Data Protection Law. University Casebook Series. University of Minnesota Law School, Foundation Press 2016.

*González Fuster, Gloria*. The Emergence of Personal Data Protection as a Fundamental Right of the EU. Springer International Publishing 2014.

*Gutwirth, Sergei – Poullet, Yves – de Hert, Paul – de Terwangne, Cecile – Nouwt, Sjaak.* Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalisation in Action. Teoksessa Reinventing Data Protection. International Law Springer 2009, s. 3—44.

*Halila, Leena*. Onko hallintoprosessilla tulevaisuutta? Lakimies 2/2016, s. 291—296.

*Hanninen, Minna – Laine, Elli – Rantala, Kati – Rusi, Mari – Varhela, Markku*. Henkilötietojen käsittely: EU-tietosuoja-asetuksen vaatimukset. Kauppakamari: Helsinki 2017.

*Heinonen, Olavi – Koskinen, Pekka – Lappi-Setälä, Tapio – Majanen, Martti – Nuotio, Kimmo – Nuutila, Ari-Matti – Rautio, Ilkka*. Rikosoikeus. (2. painos) Juva 2002.

*de Hert, Paul*. Accountability and System Responsibility: New Concepts in Data Protection Law and Human Rights Law. Tilburg University 2012.

*de Hert, Paul – Papakonstantinou, Vagelis*. The new general data protection regulation: Still a sound system for the protection of individual. Computer Law and Security Review, Volume 32, Issue 2, 2016, s. 179—194.

*Heuru, Kauko*. Kuntalaki käytännössä. Edita Oyj: Helsinki 2001.

*Hildebrandt, Mireille.* Profiling and the Identity of the European Citizen. Teoksessa Profiling the European Citizen: Cross-Disciplinary Perspective. Toim. M. Hildebrandt ja S. Gutwirth, Springer Science ja Business Media B.V. 2008, s. 303—343.

*Hollo, Erkki J.* Ennakkovalvonta ja ympäristövastuu. Suomen Ympäristötieteen Seura ry:n aikakauslehti, Ympäristöjuridiikka, toim. Aki Ekroos, N:o 103, vuosikerta 30, 3/2010, s. 3—6.

*Hällström, Minna Liisa.* Sananvapauden suhde yksityisyyden ja kunnian suojaan. Hovioikeudet, Helsinki 2004.
Saatavilla: https://oikeus.fi/hovioikeudet/helsinginhovioikeus/material/attachments/oikeus_hovioikeudet_helsinginhovioikeus/julkaisut/painetutjulkaisut/rikosoikeudenuudistuneetyleisetopit2004/NQlPX4AwB/05_Sananvapauden_suhde_yksityisyyden_ja_kunnian..._Minna-Liisa_Hallstrom.pdf
Katsottu: 28.4.2020

*Kallasvuo, Karoliina*. Omadata ja oikeus siirtää tiedot järjestelmästä toiseen. Teoksessa Viestinnän muuttuva sääntely - Viestintäoikeuden vuosikirja 2015, toim. Päivi Korpisaari, Helsinki 2016, s. 140—162.

*Karhula, Päivikki*. Paratiisi vai panoptikon?: näkökulmia ubiikkiyhteiskuntaan. Eduskunnan kirjasto, Helsinki 2008.

*Kauppi, Arto*. Potilastiedot ja poliisin tiedonhankinta: tutkimus terveydenhuollon luottamuksellisuuden suojan ja potilaan yksityisyyden suojan suhteesta poliisin potilastietoihin kohdistuviin tiedonhankintavaltuuksiin. Lapin yliopisto, julkaistu aikaisemmin Sanoma Pron kustantamana, Talentum Media cop.: Helsinki 2007.

*Kennedy, G. E. – Prabhu, L. S. P*. Data Protection Law – A Practical Guide. (2. painos) DrakeIntl 2017.

*Koillinen, Mikael*. Henkilötietojen suoja itsenäisenä perusoikeutena. Oikeus 2/2013 s. 171—193.

*Koivisto, Ida*. Oikeus on, miten se systematisoidaan? – Kysymys oikeudenalajaotuksesta ja hallinto-oikeudesta. Lakimies 7-8/2015, s. 954—972.

*Kokott, Juliane – Sobotta, Christoph*. The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR. International Data Privacy Law, Volume 3, Issue 4, 2013, s. 222—228.

*Konstari, Timo*. Asiakirjajulkisuudesta hallinnossa. Tutkimus yleisten asiakirjain julkisuudesta hallinnon kontrollivälineenä. Suomalainen lakimiesyhdistys. Vammala 1977.

*Korhonen, Anne*. Yksityisyys ja henkilötietojen suoja kunnallisessa virankäytössä. Acta nro 213. Suomen kuntaliitto verkkojulkaisu. (1. painos) Helsinki 2009.

*Korhonen, Rauno*. Perusrekisterit ja henkilötietojen suoja: Informaatio-oikeudellinen tutkimus yksityisyyden suojasta yhteiskunnan perusrekisteritietojen käsittelyssä. Acta Universitatis Lapponiensis 51. Lapin yliopisto, Rovaniemi 2003.

*Korhonen, Rauno*. Tietosuojavastaavan nimittäminen, asema ja tehtävät. Defensor Legis, 4/2016, s. 599—606.

*Korpisaari, Päivi – Pitkänen, Olli – Warma-Lehtinen, Eija*. Uusi tietosuojalainsäädäntö. Alma Talent: Helsinki 2018.

*Korte, Atte.* Kohtuuttomuus viranomaisen harkintavallan rajoitusperiaatteena – erityisesti etuosto-oikeuden näkökulmasta. Referee-artikkeli, Edilex-sarja 39/2015. Edita Publishing Oy 2015.

*Koski, Saara*. Lasten henkilötietojen suojan tehokkuus ja riittävyys Euroopan unionissa – Erityisesti esineiden internetin sovellutuksissa. Referee-artikkeli, Edilex 2017, s. 33—67.

*Koskinen, Ida*. Koneoppiminen ja EU:n yleisen tietosuoja-asetuksen vaatimus lainmukaisesta, kohtuullisesta ja läpinäkyvästä käsittelystä. Suomen asianajajaliiton oikeudellinen aikakausikirja, Defensor Legis 2/2018, s. 240—256.

*Kremer, Jens*. The New EU General Data Protection Regulation: Setting Standards for The Next Century. Liikejuridiikka 2/2016, s. 133—141.

*Kulla, Heikki – Koillinen, Mikael.* Julkisuus ja henkilötietojen suoja viranomaistoiminnassa. Turun yliopiston oikeustieteellinen tiedekunta 2014.

*Kuusikko, Kirsi*. "Oikeus hyvään hallintoon (41 artikla)". Teoksessa Perusoikeudet EU:ssa, toim. Nieminen, Liisa. Kauppakamari Oy: Jyväskylä 2001, s. 389—447.

*Linder, Andreas*. European Data Protection Law – General Data Protection Regulation, EU Commission 2016.

*Lindroos-Hovinheimo, Susanna*. Henkilötietojen suoja EU-oikeudessa – yksityisyyttä yhteisön kustannuksella? Lakimies 1/2018, s. 52—75.

*Lynskey, Orla*. The Foundations of EU Data Protection Law. OUP 2015, Oxford 2016.

*Mattila, Heikki – Kuusikko, Kirsi – Mikkola, Tuulikki – Mäkelä, Sauli – Niemi, Matti Ilari – Pöyhönen, Juho – Nystén-Haarala, Soili – Andem, Maurice N. – Juanto, Leila – Haavisto, Risto – Saarenpää, Ahti*. Oikeusjärjestys 2000: Osa 1, toim. Risto Haavisto, Lapin yliopisto (2. täydennetty painos) Rovaniemi 2002.

*Mayer-Schönberger, Viktor – Cukier, Kenneth*. Big Data: A Revolution That Will Transform How We Live, Work and Think. Toim. John Murray, Eamon Dolan ja Mariner Books 2013.

*Mäenpää, Olli*. Hallinto-oikeus. (1. painos.) (Oikeuden perusteokset). Sanoma Pro: Helsinki 2013.

*Mäenpää, Olli.* Hallintolaki ja hyvän hallinnon takeet. (3. painos), toim. Matti Lehtinen. Helsinki: Edita Publishing Oy 2008.

*Mäenpää, Olli.* Julkisuusperiaate. (3. uudistettu painos). Talentum Pro: Helsinki 2016.

*Nestlerode, Jana*. Re-Righting the Right to Privacy: The Supreme Court and the Constitutional Right to Privacy in Criminal Law. Cleveland State University, Law Journals 1993.

*Neuvonen, Riku – Rautiainen, Pauli.* Perusoikeuksien tunnistaminen ja niiden sisällön määritteleminen Suomen perusoikeusjärjestelmässä. Lakimies 1/2015, s. 28—53.

*Neuvonen, Riku.* Viestinnän metatiedot yksityisyyden suojan koetinkivenä? – Ylikansallisten tuomioistuinten ratkaisukäytännön vaikutus Suomessa. Defensor Legis 4/2016, s. 587—598.

*Neuvonen, Riku.* Yksityisyyden suoja Suomessa. Helsingin Kamari Oy 2014.

*Niemi, Johanna*. Tuomioistuinlinjat ja julkisoikeuden ja yksityisoikeuden raja-aidat. Teoksessa Matti Tolvanen – oikeustieteiden moniottelija 60 vuotta, juhlajulkaisu, toim. Altti Mieho, Edita Oyj: Helsinki 2015, s. 331—348.

*Nuotio, Kimmo*. Oikeuslähteet, "supernormistot" ja ratkaisujen perustelu. Oikeus – Kulttuuria ja teoriaa – Juhlakirja Hannu Tolonen. Turun yliopiston oikeustieteellisen tiedekunnan julkaisuja, A-julkaisut n:o 16, Turku 2005, s. 127—152.

*Nystén-Haarala, Soili – Barton, Thomas D. – Kujala, Jaakko*. Flexibility in Contracting. Rovaniemi 2015.

*Ollila, Riitta*. Henkilötietojen suoja EU:n perusoikeutena. Defensor Legis 5/2014, s. 814—824.

*Pitkänen, Olli*. Mitä lähioikeus suojaa? Lakimies 5/2017, s. 580—602.

*Pitkänen, Olli – Korpisaari, Päivi – Korhonen, Rauno*. Miten kansallista lainsäädäntöä pitää muuttaa EU:n yleisen tietosuoja-asetuksen vuoksi? Teoksessa Viestinnän muuttuva sääntely - Viestintäoikeuden vuosikirja 2016, toim. Päivi Korpisaari, Helsinki 2017, s. 1—9.

*Pitkänen, Olli – Tiilikka, Päivi – Warma, Eija*. Henkilötietojen suoja. Talentum: Helsinki 2013.

*Prosser, William L*. Privacy. California Law Review, Inc, Volume 48, Issue 3, 1960, s. 383—423.

*Pöysti, Tuomas*. Tehokkuus, informaatio ja eurooppalainen oikeusalue. Helsingin yliopiston oikeustieteellisen tiedekunnan julkaisuja. Forum Iuris. Helsinki 1999.

*Repo, Aatto J*. Tiedon arvo – muistiinpanoja I. Kirjastotiede ja informatiikka 3/1984 s. 51—60.

*Roos, Carl-Magnus*. Asiakirjojen säilytysajat. Teoksessa Säilyykö sähköinen – ja kuinka kauan? Toim. Carl-Magnus Roos, Liikearkistoyhdistys ry: Helsinki 2018, s. 100—159.

*Saarenpää, Ahti*. Henkilö- ja persoonallisuusoikeus. Teoksessa Oikeusjärjestys 2000, toim. Risto Haavisto: Osa III. (2. täydennetty painos) Lapin yliopiston oikeustieteellisiä julkaisuja. Sarja C 34. Rovaniemi 2003, s. 299—373.

*Saarenpää, Ahti*. Henkilö- ja persoonallisuusoikeus. Teoksessa Oikeus tänään, toim. Maija-Leena Niemi: Osa II. Lapin yliopiston oikeustieteellisiä julkaisuja, C-sarja n:o 63 (3. painos) Rovaniemi 2015, s. 203—430.

*Saarenpää, Ahti*. Personrätt – integritetsrätt. Teoksessa Finlands civil- och handelsrätt: En introduction, toim. Bärlund, Johan – Nybergh, Frey – Petrell, Katarina. Kauppakamari: Helsingfors 2000, s. 37—104.

*Saarenpää, Ahti*. Potilas, oikeus, ihminen – näkökohtia itsemääräämisoikeutemme suojasta. Teoksessa Oikeustiede – Jurisprudentia XXX: Suomalaisen lakimiesyhdistyksen vuosikirja. Juhlajulkaisu Aulis Aarnio. Gummerus: Helsinki 1997, s. 265—278.

*Saarenpää, Ahti – Sztobryn, Karolina*. Lawyers in the Media Society. The Legal Challenges of the Media Society. Rovaniemi 2016.

*Salokannel, Marjut*. Terveystiedot ja EU:n yleinen tietosuoja-asetus. Defensor Legis 4/2016, s. 534—548.

*Saraviita, Ilkka*. Perustuslaki. (2. uudistettu painos) Talentum: Helsinki 2011.

*Sarja, Mikko*. Yksityisyys ja julkisuus holhoustoimessa. Defensor Legis 5/2008, s. 792—820.

*Scheinin, Martin – Hallberg, Pekka – Karapuu, Heikki – Ojanen, Tuomas – Tuori, Kaarlo – Viljanen, Veli-Pekka*. Kaarlo Tuori ja Juha Lavapuro: Perusoikeuksien ja ihmisoikeuksien turvaamisvelvollisuus (PL 22 §). Teoksessa Perusoikeudet (2. uudistettu painos) (Oikeuden perusteokset), WSOYpro: Helsinki 2011, s. 809—820.

*Schellenberg, T. R – Jones H. G*. Modern Archives: Principles & Techniques. Originally published by the University of Chicago Press in 1956 and reprinted in 1975. Reissued in 2003 with a new introduction by H. G. Jones. Society of America Archivists 2003.

*Schroeter, Ulrich G.* Freedom of Contract: Comparison between provisions of the CISG (Article 6) and counterpart provisions of the PECL, The Vindobona Journal of International Commercial Law and Arbitration, Volume 6, Basel 2002, s. 257—266.

*Siitarinen, Saini*. Suomalaisen emoyhtiön vastuu ulkomaisen tytäryhtiön sosiaalisista velvoitteista – Arviointi Suomen lain näkökulmasta. Edita Publishing Oy: Edilex 2004.

*Solove, Daniel J.* A Brief History of Information Privacy Law in PROSKAUER ON PRIVACY. George Washington University Law School, GW Law Faculty Publications & Other Works 2006.

*Sorvari, Hannu*. Tiedollinen itsemääräämineninä ja markkinointi. Teoksessa Viestintäoikeus, toim. Heikki Kulla, WSOY Lakitieto: Helsinki 2002.

*Sorvari, Hannu – Lehtonen Lasse*. Geneettisen tiedon käsittelyn oikeussääntely. Teoksessa Bio-oikeus lääketieteessä, toim. Lasse Lehtonen. Helsinki 2006, s 125—149.

*Tarkela, Pekka*. Digitaalinen talous, data ja varallisuusoikeuden muutostarpeet – Property Law in Flux: How to Deal with Digital Data in Digital Economy. Liikejuridiikka 2/2016, s. 60—114.

*Tiilikka, Päivi.* Journalistin sananvapaus. Talentum Media Oy: Helsinki 2008.

*Tzanou, Maria*. Data protection as a fundamental right next to privacy? – 'Reconstructing a not so new right. International Data Privacy Law, Volume 3, Issue 2, 2013, s. 88—99.

*Tzanou, Maria*. Data Protection in EU Law: An analysis of the EU legal framework and the ECJ jurisprudence. Published online in ResearchGate 2010.

*Tzanou, Maria*. The Fundamental Right to Data Protection: Normative Value in the Context of Counter-Terrorism Surveillance. Hart Publishing: Oxford, Portland 2017.

*Van Alsenoy, Brendan*. Liability under EU Data Protection Law: From Directive 95/46 to the General Data Protection Regulation. JIPITEC, Volume 7, 2016(a).
Saatavilla: http://www.jipitec.eu/issues/jipitec-7-3-2016/4506
Katsottu: 28.4.2020

*Van Alsenoy, Brendan*. Regulating data protection: the allocation of responsibility and risk among actors involved in personal data processing. University of Leuven 2016(b).

*Voigt, Paul – Von Dem Bussche, Axel*. The EU General Data Protection Regulation (GDPR): A Practical Guide. Springer 2017.

*Voutilainen, Tomi*. ICT-oikeus sähköisessä hallinnossa – ICT-oikeudelliset periaatteet ja sähköinen hallintomenettely. Väitöskirja, Joensuun yliopisto 2009.

*Voutilainen, Tomi*. Oikeus tietoon: informaatio-oikeuden perusteet. Edita Oyj: Helsinki 2012.

*Voutilainen, Tomi*. Tietoaineistojen säilyttämisen ja arkistoimisen tietosuoja. Teoksessa Säilyykö sähköinen – ja kuinka kauan? Toim. Carl-Magnus Roos, Liikearkistoyhdistys ry: Helsinki 2018, s. 17—29.

*Voutilainen, Tomi – Galkin, Denis*. Tietosuoja pilvipalveluiden hankintasopimuksissa julkisessa hallinnossa. Defensor Legis 3/2013, s. 371—386.

*Voutilainen, Tomi – Huttunen, Kimmo*. Julkisen hallinnon tiedonhallinnan pirstaloituminen ja lainsäädäntö. Oikeus 1/2015, s. 69—81.

*Wallin, Anna-Riitta*. Henkilörekisterien käytön sääntely erityisesti asiakasrekisterien ja henkilörekisterien kannalta. Helsinki 1991.

*Wallin, Anna-Riitta*. Tiedonsaanti asiakirjoista ja henkilötietojen suoja EU:n perusoikeuskirjassa tunnustettuina perusoikeuksina. Teoksessa Perusoikeudet EU:ssa, toim. Nieminen, Liisa. Kauppakamari Oy: Helsinki 2001, s. 351—387.

*Wallin, Anna-Riitta*. Yritystoiminnan ja julkishallinnon avoimuus informaatio- ja viestintäoikeudellisesta näkökulmasta. Viestintäoikeus, toim. Heikki Kulla, WSOY Lakitieto: Helsinki 2002, s. 123—146.

*Wasserstrom, Richard A*. Privacy: Some Arguments and Assumptions. Teoksessa Philosophical Law: Authority, Equality, Adjudication, Privacy, toim. Richard Bronaugh. Greenwood Press: Westport 1978, s. 148—166.

*Weiss, Martin A. – Archick, Kristin*. U.S.-EU Data Privacy: From Safe Harbor to Privacy Shield. Congressional Research Service 2016.

*Wennäkoski, Anna Aurora*. Tietosuojaoikeudellinen vahingonkorvaus murroksessa. Teoksessa Viestinnän muuttuva sääntely - Viestintäoikeuden vuosikirja 2016, toim. Päivi Korpisaari, Helsinki 2017, s. 68—91.

*Wilhelmsson, Thomas*. Yksityisoikeuden uudet mahdollisuudet. Teoksessa Pieniä kertomuksia hyvinvointivaltion siviilioikeudesta, toim. Thomas Wilhelmsson, Werner Söderström Lakitieto Oy: Helsinki 2000, s. 19—44.

# Virallislähteet

## Eurooppaoikeudelliset säädökset ja kansainväliset sopimukset

*Arkistoasetus.* Euroopan talousyhteisön ja Euroopan atomienergiayhteisön historiallisten arkistojen avaamisesta yleisölle 1.2.1983 annettu neuvoston asetus (ETY, Euratom) N:o 354/83.
Saatavilla: https://eur-lex.europa.eu/legal-content/FI/ALL/?uri=CELEX:31983R0354
Katsottu: 29.4.2020

*Bryssel I -asetus.* Euroopan parlamentin ja neuvoston asetus (EU) N:o 1215/2012, annettu 12.12.2012, tuomioistuimen toimivallasta sekä tuomioiden tunnustamisesta ja täytäntöönpanosta siviili- ja kauppaoikeuden alalla (*Bryssel I*).
Saatavilla: https://eur-lex.europa.eu/legal-content/FI/ALL/?uri=CELEX%3A32012R1215
Katsottu: 29.4.2020

*Convention for the protection of individuals with regard to automatic processing of personal data 1.10.1985*. Council of Europe, European Treaty Services No. 108, SopS 32/1992. Yksi todistusvoimaisista kielistä on englanti, joten käytän lähteenä linkin kautta aukeavaa alkuperäistä englanninkielistä sopimusta.
Saatavilla: https://rm.coe.int/1680078b37
Katsottu: 29.4.2020

*Direktiivi julkisista hankinnoista*. Euroopan parlamentin ja neuvoston direktiivi 2014/24/EU, annettu 26.2.2014, julkisista hankinnoista ja direktiivin 2004/18/EY kumoamisesta.
Saatavilla: https://eur-lex.europa.eu/legal-content/FI/TXT/?uri=celex%3A32014L0024
Katsottu: 29.4.2020

*Direktiivi sähköisestä kaupankäynnistä*. Euroopan parlamentin ja neuvoston direktiivi 2000/31/EY, annettu 8.6.2000, tietoyhteiskunnan palveluja, erityisesti sähköistä kaupankäyntiä, sisämarkkinoilla koskevista tietyistä oikeudellisista näkökohdista.
Saatavilla: https://eur-lex.europa.eu/legal-content/FI/ALL/?uri=CELEX:32000L0031
Katsottu: 29.4.2020

*EASA-asetus.* Euroopan parlamentin ja neuvoston asetus (EY) N:o 216/2008, annettu 20.2.2008, yhteisistä siviili-ilmailua koskevista säännöistä ja Euroopan lentoturvallisuusviraston perustamisesta sekä neuvoston direktiivin 91/670/ETY, asetuksen (EY) N:o 1592/2002 ja direktiivin 2004/36/EY kumoamisesta.
Saatavilla: https://eur-lex.europa.eu/legal-content/FI/TXT/?uri=CELEX%3A32008R0216
Katsottu: 1.5.2020

*EU:n toimintaa koskeva tietosuoja-asetus*. Euroopan parlamentin ja neuvoston asetus (EU) 2018/1725, annettu 23.10.2018, luonnollisten henkilöiden suojelusta unionin toimielinten, elinten ja laitosten suorittamassa henkilötietojen käsittelyssä ja näiden tietojen vapaasta liikkuvuudesta sekä asetuksen (EY) N:o 45/2001 ja päätöksen N:o 1247/2002/EY kumoamisesta.
Saatavilla: https://eur-lex.europa.eu/legal-content/FI/TXT/?uri=CELEX%3A32018R1725
Katsottu: 29.4.2020

*Euroopan hyvän hallintotavan säännöstä*, 1.3.2002.
Saatavilla: https://www.ombudsman.europa.eu/fi/publication/fi/3510
Katsottu: 29.4.2020

*Euroopan ihmisoikeussopimus* (Yleissopimus ihmisoikeuksien ja perusvapauksien suojaamiseksi, EIS) sellaisena kuin se on muutettuna yhdennellätoista pöytäkirjalla SopS 63/1999.
Saatavissa: https://www.finlex.fi/fi/sopimukset/sopsteksti/1999/19990063#idp450499008
Katsottu 29.4.2020

*Euroopan julkisuusasetus*. Euroopan parlamentin ja neuvoston asetus (EY) N:o 1049/2001, annettu 30.5.2001, Euroopan parlamentin, neuvoston ja komission asiakirjojen saamisesta yleisön tutustuttavaksi.
Saatavilla: https://eur-lex.europa.eu/legal-content/FI/ALL/?uri=CELEX%3A32001R1049
Katsottu: 29.4.2020

*Euroopan parlamentin ja neuvoston asetus (EU) N:o 910/2014,* annettu 23.7.2014, sähköisestä tunnistamisesta ja sähköisiin transaktioihin liittyvistä luottamuspalveluista sisämarkkinoilla ja direktiivin 1999/93/EY kumoamisesta.
Saatavilla: https://eur-lex.europa.eu/legal-content/FI/TXT/?uri=CELEX%3A32014R0910
Katsottu: 29.4.2020

*Euroopan parlamentin ja neuvoston direktiivi (EU) 2016/680*, annettu 27.4.2016, luonnollisten henkilöiden suojelusta toimivaltaisten viranomaisten suorittamassa henkilötietojen käsittelyssä rikosten ennalta estämistä, tutkimista, paljastamista tai rikoksiin liittyviä syytetoimia tai rikosoikeudellisten seuraamusten täytäntöönpanoa varten sekä näiden tietojen vapaasta liikkuvuudesta ja neuvoston puitepäätöksen 2008/977/YOS kumoamisesta.
Saatavilla: https://eur-lex.europa.eu/legal-content/FI/TXT/?uri=CELEX%3A32016L0680
Katsottu: 29.4.2020

*Euroopan unionin perusoikeuskirja* 2012/C 326/02.
Saatavissa: http://eur-lex.europa.eu/legal-content/FI/TXT/HTML/?uri=CELEX:12012P/TXT&from=FI
Katsottu 29.4.2020

*Euroopan unionista tehdyn sopimuksen ja Euroopan unionin toiminnasta tehdyn sopimuksen konsolidoidut toisinnot (SEU ja SEUT)* (2016/C 202/01).
Saatavissa: https://eur-lex.europa.eu/legal-content/FI/TXT/HTML/?uri=OJ:C:2016:202:FULL&from=EN
Katsottu: 29.4.2020

*Henkilötietodirektiivi*. Euroopan parlamentin ja neuvoston direktiivi 95/46/EY annettu 24.10.1995, yksilöiden suojelusta henkilötietojen käsittelyssä ja näiden tietojen vapaasta liikkuvuudesta.
Saatavilla: http://eur-lex.europa.eu/legal-content/FI/TXT/?uri=CELEX:31995L0046
Katsottu: 29.4.2020

*Kansalaisoikeuksia ja poliittisia oikeuksia koskeva kansainvälinen yleissopimus (KP-sopimus)*, SopS 8/1976 (Yhdistyneet kansakunnat, YK).

*Maastrichtin sopimus*. Sopimus Euroopan unionista OJ C 191, 29.7.1992, s. 1-112 (ES, DA, DE, EL, EN, FR, GA, IT, NL. PT).
Saatavilla: https://eur-lex.europa.eu/legal-content/FI/TXT/?uri=celex:11992M/TXT
Katsottu: 29.4.2020

*Matkustajarekisteridirektiivi*. Euroopan parlamentin ja neuvoston direktiivi (EU) 2016/681, annettu 27.4.2016, matkustajarekisteritietojen (PNR) käytöstä terroririkosten ja vakavan rikollisuuden ennalta ehkäisemistä, paljastamista ja tutkintaa sekä tällaisiin rikoksiin liittyviä syytetoimia varten.
Saatavilla: https://eur-lex.europa.eu/legal-content/fi/TXT/?uri=CELEX:32016L0681
Katsottu: 29.4.2020

*Rooma II -asetus*. Euroopan parlamentin ja neuvoston asetus (EY) N:o 864/2007, annettu 11.7.2007, sopimukseen perustumattomiin velvoitteisiin sovellettavasta laista (*Rooma II*).
Saatavilla: https://eur-lex.europa.eu/legal-content/FI/ALL/?uri=CELEX:32007R0864
Katsottu: 29.4.2020

*Sähköisen viestinnän tietosuoja direktiivi*. Euroopan parlamentin ja neuvoston direktiivi 2002/58/EY, annettu 12.7.2002, henkilötietojen käsittelystä ja yksityisyyden suojasta sähköisen viestinnän alalla.
Saatavilla: https://eur-lex.europa.eu/legal-content/fi/ALL/?uri=CELEX:32002L0058
Katsottu: 29.4.2020

*Tietosuojasopimus,* SopS 36/1992. Ratifioitu Suomessa asetuksella yksilöiden suojelemista henkilötietojen automaattisessa tietojenkäsittelyssä koskevan yleissopimuksen voimaansaattamisesta sekä yleissopimuksen eräiden määräysten hyväksymisestä annetun lain voimaantulosta. 1.4.1992, Euroopan neuvoston ”*tietosuojasopimus*”.

*Verkko- ja tietojärjestelmädirektiivi*. Euroopan parlamentin ja neuvoston direktiivi (EU) 2016/1148, annettu 6.7.2016, toimenpiteistä yhteisen korkeatasoisen verkko- ja tietojärjestelmien turvallisuuden varmistamiseksi koko unionissa.
Saatavilla: https://eur-lex.europa.eu/legal-content/FI/ALL/?uri=CELEX%3A32016L1148
Katsottu: 29.4.2020

*Yleinen tietosuoja-asetus (GDPR)*. Euroopan parlamentin ja neuvoston asetus (EU) 2016/679 annettu 27.4.2016, luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta.
Saatavilla: http://eur-lex.europa.eu/legal-content/FI/TXT/?uri=CELEX%3A32016R0679
Katsottu: 29.4.2020

**Ulkomainen lainsäädäntö**

*IV Amendment*. The Fourth Amendment to the United States Constitution. Part of the Bill of Rights. Search and Seizure. Passed by Congress Sep. 25, 1789. Ratified Dec. 15, 1791 / Yhdysvallat.

*V Amendment*. The Fifth Amendment to the United States Constitution, part of the Bill of Right, that articulates procedural safeguards designed to protect the right of the criminally accused and to ensure life, liberty and property. Ratified in 1791 / Yhdysvallat.

*Communication Act of 1934*. U.S. federal law signed by President Franklin D. Roosevelt on June 19, 1934 and codified as Chapter 5 of Title 47 of the United States Code, 47 U.S.C. § 151 et seq / Yhdysvallat.

*U.S. Code: 42 U.S. Code § 1702*. Yhdysvaltain liittovaltion laki vuodelta 1825, joka löytyy nykyisin kohdasta (otsikon 18 Crimes and Criminal Procedure alta) 18 U.S. Code § 1702. Obstruction of correspondence. (June 15, 1948, ch. 645, 62 Stat. 778; Pub. L. 103-322, title XXXIII, § 330016(1)(I), Sept. 13, 1994, 108 Stat. 2147.) / Yhdysvallat.

*U.S. Constitution*. Constitution of the United States of America, the fundamental law of the U.S. federal system of government. Written during the summer of 1787 in Philadelphia by 55 delegates to a Constitutional Convention called ostensibly to amend the Articles of Confederation (1781-1789). Ratified in 1792 as the Twenty-seventh Amendment / Yhdysvallat.

**Hallituksen esitykset**

*HE 84/1974 vp*. Hallituksen esitys eduskunnalle laeiksi 1) rikoslain 27 luvun, 2) painovapauslain 18 ja 39 §:n sekä 3) oikeudenkäytön julkisuudesta annetun lain 1 ja 2 §:n muuttamisesta. Helsinki 1974.
Saatavilla: https://www.eduskunta.fi/FI/vaski/HallituksenEsitys/Documents/he_84+1974.pdf
Katsottu: 29.4.2020

*HE 49/1986 vp*. Hallituksen esitys eduskunnalle henkilörekisterilaiksi ja siihen liittyviksi laeiksi. Helsinki 1986.
Saatavilla: https://www.eduskunta.fi/FI/vaski/HallituksenEsitys/Documents/he_49+1986.pdf
Katsottu: 29.4.2020

*HE 309/1993 vp*. Hallituksen esitys eduskunnalle perustuslakien perusoikeussäännösten muuttamisesta. Helsinki 1993.
Saatavilla: https://www.eduskunta.fi/FI/vaski/HallituksenEsitys/Documents/he_309+1993.pdf
Katsottu: 29.4.2020

*HE 311/1993 vp*. Hallituksen esitys eduskunnalle laeiksi henkilörekisterilain ja yleisten asiakirjain julkisuudesta annetun lain 18 a §:n muuttamisesta sekä laiksi tietosuojalautakunnasta ja tietosuojavaltuutetusta. Helsinki 1993.
Saatavilla: https://www.eduskunta.fi/FI/vaski/HallituksenEsitys/Documents/he_311+1993.pdf
Katsottu: 29.4.2020

*HE 239/1997 vp*. Hallituksen esitys eduskunnalle yksityisyyden, rauhan ja kunnian loukkaamista koskevien rangaistussäännösten uudistamiseksi. Helsinki 1997.
Saatavilla: https://www.eduskunta.fi/FI/vaski/HallituksenEsitys/Documents/he_239+1997.pdf
Katsottu: 29.4.2020

*HE 30/1998 vp*. Hallituksen esitys eduskunnalle laiksi viranomaisten toiminnan julkisuudesta ja siihen liittyviksi laeiksi. Helsinki 1998.
Saatavilla: https://www.eduskunta.fi/FI/vaski/HallituksenEsitys/Documents/he_30+1998.pdf
Katsottu: 29.4.2020

*HE 96/1998 vp*. Hallituksen esitys eduskunnalle henkilötietolaiksi ja eräiksi siihen liittyviksi laeiksi. Helsinki 1998.
Saatavilla: https://www.eduskunta.fi/FI/vaski/HallituksenEsitys/Documents/he_96+1998.pdf
Katsottu: 29.4.2020

*HE 184/1999 vp*. Hallituksen esitys eduskunnalle yksityisyyden, rauhan ja kunnian loukkaamista koskevien rangaistussäännösten uudistamiseksi. Helsinki 1999.
Saatavilla: https://www.eduskunta.fi/FI/vaski/HallituksenEsitys/Documents/he_184+1999.pdf
Katsottu: 29.4.2020

*HE 75/2011 vp*. Hallituksen esitys eduskunnalle laeiksi sairausvakuutuslain ja työterveyshuoltolain muuttamisesta. Helsinki 2011.
Saatavilla: https://www.eduskunta.fi/FI/vaski/HallituksenEsitys/Documents/he_75+2011.pdf
Katsottu: 29.4.2020

*HE 9/2018 vp*. Hallituksen esitys eduskunnalle EU:n yleistä tietosuoja-asetusta täydentäväksi lainsäädännöksi. Helsinki 2018.
Saatavilla: https://www.eduskunta.fi/FI/vaski/HallituksenEsitys/Documents/HE_9+2018.pdf
Katsottu: 29.4.2020

*HE 55/2018 vp*. Hallituksen esitys eduskunnalle laiksi lentoliikenteen matkustajarekisteritietojen käytöstä terrorismin ja vakavan rikollisuuden torjunnassa sekä eräiksi siihen liittyviksi laeiksi. Helsinki 2018.
Saatavilla: https://www.eduskunta.fi/FI/vaski/HallituksenEsitys/Documents/HE_55+2018.pdf
Katsottu: 29.4.2020

*HE 2/2020 vp*. Hallituksen esitys eduskunnalle laeiksi oikeusministeriön hallinnonalan eräiden henkilötietojen käsittelyä koskevien säännösten muuttamisesta. Helsinki 2020.
Saatavilla: https://www.eduskunta.fi/FI/vaski/HallituksenEsitys/Documents/HE_2+2020.pdf
Katsottu: 29.4.2020

**Eduskunnan valiokuntien lausunnot ja mietinnöt**

*PeVL 7/1997 vp*. Perustuslakivaliokunnan lausunto 7/1997 vp hallituksen esityksestä 20/1997 vp (HE 20/1997 vp).
Saatavilla: https://www.eduskunta.fi/FI/vaski/Lausunto/Documents/pevl_7+1997.pdf
Katsottu: 29.4.2020

*PeVL 11/1997 vp*. Perustuslakivaliokunnan lausunto 11/1997 vp hallituksen esityksestä 49/1997 vp (HE 49/1997 vp).
Saatavilla: https://www.eduskunta.fi/FI/vaski/Lausunto/Documents/pevl_11+1997.pdf
Katsottu: 29.4.2020

*PeVL 25/1998 vp*. Perustuslakivaliokunnan lausunto 25/1998 vp hallituksen esityksestä henkilötietolaiksi ja eräiksi siihen liittyviksi laeiksi (HE 96/1998 vp).
Saatavilla: https://www.eduskunta.fi/FI/vaski/Lausunto/Documents/pevl_25+1998.pdf
Katsottu: 29.4.2020

*PeVL 51/2002 vp*. Perustuslakivaliokunnan lausunto 51/2002 vp hallituksen esityksestä laiksi henkilötietojen käsittelystä poliisitoimessa ja eräiksi siihen liittyviksi laeiksi (HE 93/2002 vp).
Saatavilla: https://www.eduskunta.fi/FI/vaski/Lausunto/Documents/pevl_51+2002.pdf
Katsottu: 29.4.2020

*PeVL 25/2005 vp*. Perustuslakivaliokunnan lausunto 25/2005 vp hallituksen esityksestä laiksi tilatukijärjestelmän täytäntöönpanosta (HE 17/2005 vp).
Saatavilla: https://www.eduskunta.fi/FI/vaski/Lausunto/Documents/pevl_25+2005.pdf
Katsottu: 29.4.2020

*PeVL 20/2006 vp*. Perustuslakivaliokunnan lausunto 20/2006 vp hallituksen esityksestä laiksi tilatukijärjestelmän täytäntöönpanosta annetun lain muuttamisesta (HE 37/2006 vp).
Saatavilla: https://www.eduskunta.fi/FI/vaski/Lausunto/Documents/pevl_20+2006.pdf
Katsottu: 29.4.2020

*PeVL 11/2008 vp*. Perustuslakivaliokunnan lausunto 11/2008 vp: Valtioneuvoston kirjelmä ehdotuksesta neuvoston puitepäätökseksi matkustajarekisterin käytöstä lainvalvontatarkoituksiin (matkustajarekisterin käyttö lainvalvontatarkoituksiin).
Saatavilla: https://www.eduskunta.fi/FI/vaski/Lausunto/Documents/pevl_11+2008.pdf
Katsottu: 29.4.2020

*PeVM 25/1994 vp*. Perustuslakivaliokunnan mietintö n:o 25 hallituksen esityksestä perustuslakien perusoikeussäännösten muuttamisesta. Helsinki 1994.
Saatavilla: https://www.eduskunta.fi/FI/vaski/Mietinto/Documents/pevm_25+1994.pdf
Katsottu: 29.4.2020

**Standardit ja suositukset**

*ISO/IEC 27001:2013 -standardi*. European Standard EN ISO/IEC 27001:2017 "Information technology. Security techniques. Information security management systems. Requirements (ISO/IEC 27001:2013 including Cor 1:2014 and Cor 2:2015). Eurooppalainen standardi EN ISO/IEC 27001:2017 on vahvistettu suomalaiseksi kansalliseksi standardiksi, jota auditoi Suomen Standardisoimisliitto SFS ry. Englannin kielinen versio on vahvistettu 3.3.2017. Suomenkielinen versio vahvistettiin 10.3.2017. SFS/ICS 03.100.70; 35.030. (ISO, International Organization for Standardization; IEC, International Electrotechnical Commission).

*Kansallinen turvallisuusauditointikriteeristö (Katakri 2015)*. Puolustusministeriön johdolla laadittu tietoturvallisuuden auditointityökalu viranomaisille. Katakri 2015 auditointityökalu on hyväksytty käyttöön NSA:n (National Security Agency eli Yhdysvaltain kansallinen turvallisuusvirasto) yhteistyöryhmässä 26.3.2015.
Saatavilla: https://www.defmin.fi/files/3165/Katakri_2015_Tietoturvallisuuden_auditointityokalu_viranomaisille.pdf
Katsottu 29.4.2020

**Muut**

*Annex to Opinion 3/2015*: Comparative table of GDPR texts with EDPS recommendations. Article 6 and 22. (EDPS).
Saatavilla: https://edps.europa.eu/sites/edp/files/publication/15-07-27_gdpr_recommendations_annex_en_1.pdf
Katsottu: 29.4.2020

*Article 29 Data Protection Working Party, WP 169*. Opinion 1/2010 on the concepts of "controller and "processor". 00254/10/EN, WP 169, 16.2.2010.
Saatavilla: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_en.pdf
Katsottu: 29.4.2020

*Article 29 Data Protection Working Party, WP 173*. Opinion 3/2010 on the principle of accountability. 00062/10/EN WP 173, 13.7.2010.
Saatavilla: http://www.dataprotection.ro/servlet/ViewDocument?id=654
Katsottu: 29.4.2020

*Article 29 Data Protection Working Party, WP 203*. WP-29's Opinion 03/2013 on purpose limitation. 00569/13/EN, WP 203, 2.4.2013.
Saatavilla: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf
Katsottu: 29.4.2020

*Article 29 Data Protection Working Party, WP 236*. Statement on the 2016 action plan for the implementation of the General Data Protection Regulation (GDPR). 442/16/EN WP 236, 2.2.2016.
Saatavilla: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2016/wp236_en.pdf
Katsottu: 29.4.2020

*Article 29 Data Protection Working Party, WP 244*. Guidelines for identifying a controller or processor's lead supervisory authority. 16/EN, WP 244, 13.12.2016.
Saatavilla: http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp244_en_40857.pdf
Katsottu: 29.4.2020

*Article 29 Data Protection Working Party, WP 250*. Guidelines on Personal data breach notification under Regulation 2016/679. 18/EN, WP 250 rev. 01, 3.10.2017.
Saatavilla: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052
Katsottu: 29.4.2020

*Article 29 Data Protection Working Party, WP 260*. Guideline on transparency under Regulation 2016/679. 17/EN WP260 rev. 01, 22.08.2018.
Saatavilla: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227
Katsottu: 29.4.2020

*Article 29 Data Protection Working Party, WP 263*. Working Document Setting a Co-Operation Procedure for approval of "Binding Corporate Rules" for controller and processor under GDPR. 17/EN, WP 263 rev. 01, 11.4.2018.
Saatavilla: https://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=51310
Katsottu: 29.4.2020

*ASEAN:n ihmisoikeusjulistus*. ASEAN Human Rights Declaration and the Phnom Penh Statement on the Adoption of the ASEAN Human Rights Declaration (AHRD).
Saatavilla: https://www.asean.org/storage/images/ASEAN_RTK_2014/6_AHRD_Booklet.pdf
Katsottu: 29.4.2020

*COM(2013) 847 final*. European Commission, Brussels, 27.11.2013 COM(2013) 847 final. Communication from the commission to the European parliament and the Council on the Functioning of the Safe Harbour from the Perspective of EU Citizens and Companies Established in the EU.
Saatavilla: https://ec.europa.eu/transparency/regdoc/rep/1/2013/EN/1-2013-847-EN-F1-1.Pdf
Katsottu: 29.4.2020

*COM(2016) 4176 final*. European Commission, Brussels, 12.7.2016 C(2016) 4176 final. Commission implementing decision of 12.7.2016 pursuant to Directive of the European Parliament and the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield.
Saatavilla: http://www.statewatch.org/news/2016/jul/eu-usa-com-privacy-shield-adequacy-decision.pdf
Katsottu: 29.4.2020

*Committee on Civil Liberties, Justice and Home Affairs on the GDPR (LIBE on the GDPR)*. Protection of individuals with regard to the processing of personal data. European Parliament legislative resolution of 12 March 2014 on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (COM(2012)0011 — C7-0025/2012 — 2012/0011(COD)) P7_TA(2014)0212.
Saatavilla: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52014AP0212&from=EN
Katsottu: 29.4.2020

*Digitaalisten sisämarkkinoiden -strategia (DSM-strategia)*. Commission staff working document: A Digital Sigle Market Strategy for Europe – Analysis and Evidence Accompanying the document Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions A Digital Single Market Strategy for Europe. Brussels, 6.5.2015 SWD(2015) 100 final COM(2015) 192 final.
Saatavilla: https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX:52015SC0100
Katsottu: 29.4.2020

*Ehdotus sähköisen viestinnän tietosuoja-asetukseksi*. Ehdotus Euroopan parlamentin ja neuvoston asetukseksi yksityiselämän kunnioittamisesta ja henkilötietojen suojasta sähköisessä viestinnässä ja direktiivin 2002/58/EY kumoamisesta. Euroopan komissio, Bryssel 10.1.2017 COM(2017) 10 final, 2017/0003(COD).
Saatavilla: https://eur-lex.europa.eu/legal-content/FI/TXT/?uri=CELEX%3A52017PC0010
Katsottu: 29.4.2020

*EU:n perusoikeuskirjan soveltamista koskeva kertomus vuodesta 2014*. Komission kertomus Euroopan parlamentille, neuvostolle, Euroopan talous- ja sosiaalikomitealle ja alueiden komitealle EU:n perusoikeuskirjan soveltamisesta, Bryssel 8.5.2015 SWD (2015) 99 final.
Saatavilla: http://ec.europa.eu/transparency/regdoc/rep/1/2015/FI/1-2015-191-FI-F1-1.PDF
Katsottu: 29.4.2020

*European Parliament on the GDPR*. Protection of individuals with regard to the processing of personal data. European Parliament legislative resolution of 12 March 2014 on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (COM(2012)0011 — C7-0025/2012 — 2012/0011(COD)) P7_TA(2014)0212.
Saatavilla: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52014AP0212&from=EN
Katsottu: 29.4.2020

*Guide to the EU-U.S. Privacy Shield*. European Commission 2016.
Saatavilla: https://ec.europa.eu/info/sites/info/files/2016-08-01-ps-citizens-guide_en.pd_.pdf
Katsottu: 29.4.2020

*Handbook on European data protection law*. European Union Agency for Fundamental Rights, Council of Europe, European Data Protection Supervisor, European Court of Human Rights. Publications Office of the EU 2018.
Saatavilla: https://op.europa.eu/en/publication-detail/-/publication/5b0cfa83-63f3-11e8-ab9c-01aa75ed71a1/language-en
Katsottu: 29.4.2020

*Henkilötietojen suojaamisesta maksutapahtumissa annettu suositus R(90) 19/13.9.1990*, (EN, Euroopan neuvosto). Council of Europe, Committee of Ministers: Recommendation No. R (90) 19 of the Committee of Ministers to Member States on the Protection of Personal Data Used for Payment and Other Related Operations 13.9.1990 at the 443rd meeting of the Ministers' Deputies.
Saatavilla: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016804e15cd
Katsottu: 29.4.2020

*Ihmisoikeuksien yleismaailmallinen julistus* (YK) annettu 10.12.1948 (engl. Universal Declaration of Human Rights, UDHR).
Saatavilla: https://www.un.org/en/udhrbook/pdf/udhr_booklet_en_web.pdf
Katsottu: 29.4.2020

*Liikenne- ja viestintäministeriö, 4/2016*. Liikenne ja viestintäministeriö: Maailman luotetuinta digitaalista liiketoimintaa. Työryhmän ehdotus Suomen tietoturvallisuusstrategiaksi, Liikenne- ja viestintäministeriön julkaisuja 4/2016. Julkaistu 10.2.2016.
Saatavilla: http://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/75319/Julkaisuja%204-2016.pdf?sequence=1&isAllowed=y
Katsottu: 29.4.2020

*Oikeusministeriön julkaisu, 11/2006*. Lainlaatijan perustuslakiopas, julkaisu 2006:11. Oikeusministeriö: Helsinki 2.10.2006.
Saatavilla: https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/75984/11_2006_lainlaatijan_perustuslakiopas_98_s.pdf?sequence=1&isAllowed=y
Katsottu: 29.4.2020

*Oikeusministeriön selvityksiä ja ohjeita, 4/2017*. Miten valmistautua EU:n tietosuoja-asetukseen? 1.3.2017.
Saatavilla: http://www.tietosuoja.fi/material/attachments/tietosuojavaltuutettu/-tietosuojavaltuutetuntoimisto/oppaat/1Em8rT7IF/Miten_valmistautua_EUn_tietosuoja-asetukseen.pdf
Katsottu: 29.4.2020

*Olli Mäenpään lausunto perustuslakivaliokunnalle, 6.2.2019*. Lausunto perustuslakivaliokunnalle liittyen hallituksen esitykseen laiksi julkisen hallinnon tiedonhallinnasta sekä eräiksi siihen liittyviksi laeiksi (HE 284/2018 vp.).
Saatavilla: https://www.eduskunta.fi/FI/vaski/JulkaisuMetatieto/Documents/EDK-2019-AK-243634.pdf
Katsottu: 29.4.2020

*Poliisitoimen tietosuojaa koskeva suositus R(87) 15/17.9.1987*, (EN, Euroopan neuvosto). Council of Europe, Committee of Ministers: Recommendation No. R (87) 15 of the Committee of Ministers to Member States Regulating the Use of Personal Data in the Police Sector 17.9.1987 at the 410th meeting of the Ministers' Debuties.
Saatavilla: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016804e7a3c
Katsottu: 29.4.2020

*Privacy Shieldin liite I*. EU-U.S. Privacy Shield Framework Principles Issued by the U.S. Department of Commerce: Annex I.
Saatavilla: https://www.privacyshield.gov/servlet/servlet.FileDownload?file=015t00000004qAg
Katsottu: 29.4.2020

*Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of the Personal Data, 23.9.1980.* (OECD, Organisation for Economic Co-operation and Development).
Saatavilla: https://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm
Katsottu: 29.4.2020

*Sosiaaliturvan tietosuojaa koskeva suositus R(86) 1/23.1.1986*, (EN; Euroopan neuvosto). Council of Europe, Committee of Ministers: Recommendation No. R (86) 1 of the Committee of Ministers to Member States on the Protection of Personal Data Used for Social Security Purposes 23.1.1986 at the 392nd meeting of the Ministers' Deputies.
Saatavilla: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016804dd352
Katsottu: 29.4.2020

*Suoramarkkinointia koskeva suositus R(85) 20/25.10.1985*, (EN, Euroopan neuvosto). Council of Europe, Committee of Ministers: Recommendation No. R (85) 4 of the Committee of Ministers to Member States on the Protection of Personal Data Used for the Purposes of Direct Marketing 25.10.2985 at the 389th meeting of the Ministers' Deputies.
Saatavilla: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016804bd336
Katsottu 29.4.2020

*TATTI-mietintö 35/2017*. Oikeusministeriön mietintö ja lausunto, EU:n yleisen tietosuoja-asetuksen täytäntöönpanotyöryhmän (TATTI) mietintö 35/2017.
Saatavilla: https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/80098/OMML_35_2017_EUn_ yleinen_tietosuoja.pdf?sequence=1
Katsottu: 29.4.2020

*Tietosuojatyöryhmä, WP 248*. Tietosuojatyöryhmän ohjeet tietosuojaa koskevasta vaikutustenarvioinnista ja keinoista selvittää ”liittyykö käsittelyyn todennäköisesti” asetuksessa (EU) 2016/679 tarkoitettu ”korkea riski”. 17/FI, WP 248 rev. 01, Annettu 4.4.2017 ja viimeksi tarkistettu ja hyväksytty 4.10.2017.
Saatavilla: https://tietosuoja.fi/documents/6927448/8316711/Vaikutustenarviointi+fi.pdf/af51e999-5326-4223-9deb-e21bdd2e0a63/Vaikutustenarviointi+fi.pdf
Katsottu: 29.4.2020

*Tietosuojatyöryhmä, WP 251*. Tietosuojatyöryhmän suuntaviivoja automatisoiduista yksittäispäätöksistä ja profiloinnista asetuksen (EU) 2016/679 täytäntöön panemiseksi. 17/FI, WP 251 rev. 01, Annettu 3.10.2017 ja viimeksi tarkistettu sekä hyväksytty 6.2.2018.
Saatavilla: https://tietosuoja.fi/documents/6927448/8316711/Automaattinen+p%C3%A4%C3%A4t%C3%B6ksenteko/28ae24f4-3345-4fb2-8708-c84abd8f57b0/Automaattinen+p%C3%A4%C3%A4t%C3%B6ksenteko.pdf
Katsottu: 29.4.2020

*Tietosuojavaltuutetun toimiston ohje (2010)*. Rekisteritutkimuksen tietosuojaopas tutkijoille ja tietopyyntöjä käsitteleville viranomaisille. 27.7.2010.
Saatavilla: https://tietosuoja.fi/documents/6927448/10594424/Rekisteritutkimuksen+tietosuojaopas/dd6cd081-1557-6f77-8794-5edc8555c557/Rekisteritutkimuksen+tietosuojaopas.pdf
Katsottu: 29.4.2020

*Työelämää koskeva suositus R(89) 2/18.1.1989*, (EN, Euroopan neuvosto). Council of Europe, Committee of Ministers: Recommendation No. R (89) 2 of the Committee of Ministers to Member States on the Protection of Personal Data Used for Employment Purposes 18.1.1989 at the 423rd meeting of the Ministers' Deputies.
Saatavilla: https://www.coe.int/t/dg3/healthbioethic/texts_and_documents/Rec(89)2E.pdf
Katsottu: 29.4.2020

*VAHTI, 7/2013*. Vahtiohje: Valtiovarainministeriön alaisen valtionhallinnon tietoturvallisuuden johtoryhmän (VAHTI) ohje riskien arvioinnista tietoturvallisuuden edistämiseksi valtionhallinnossa, 7/2013, Valtionvarainministeriön hallinnon kehittämisosasto. VM 41/01/2003, Ohje 3.12.2003, ministeriöille, virastoille ja laitoksille.
Saatavilla: https://www.vahtiohje.fi/c/document_library/get_file?uuid=d1bcc4b1-789e-4ce1-a44a-e591a60985b5&groupId=10229
Katsottu: 29.4.2020

*VAHTI, 1/2016*. Valtiovarainministeriön alaisen valtionhallinnon tietoturvallisuuden johtoryhmän (VAHTI) VAHTI-raportti, 1/2016: EU-tietosuojan kokonaisuudistus.
Saatavilla: https://www.vahtiohje.fi/c/document_library/get_file?uuid=ddb05959-40d1-435f-af23-fd20fc21d63f&groupId=10229
Katsottu: 29.4.2020

*Valtioneuvoston periaatepäätös, 24.1.2013*. Suomen kyberturvallisuusstrategia.
Saatavilla: https://puolustusvoimat.fi/documents/2182700/0/Kyberturvallisuusstrategia/bb56d179-9b3a-4816-806d-84c84b04da30
Katsottu: 29.4.2020

# Oikeuskäytäntö

## Euroopan ihmisoikeustuomioistuimen ratkaisut

*Biriuk v. Liettua*. Application no. 23373/03 (25.11.2008) (Final 25.02.2009).
Saatavilla: https://hudoc.echr.coe.int/app/conversion/pdf/?library=ECHR&id=003-2558775-2780393&filename=003-2558775-2780393.pdf&TID=thkbhnilzk
Katsottu: 29.4.2020

*Colombani, Incyan ja Le Monde v. Ranska*. Application no. 51279/99 (25.6.2002).
Information Note on the Court's case-law No. 43. Englanninkielinen tiivistelmä ranskaksi julkaistusta ratkaisusta.
Saatavilla: https://hudoc.echr.coe.int/eng#{"itemid":["002-5314"]}
Katsottu: 29.4.2020

*Jussila v. Suomi*, Application no. 73053/01 (23.11.2006).
Saatavilla: https://www.refworld.org/pdfid/5242c1924.pdf
Englanninkielinen tiivistelmä saatavilla: https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22002-3041%22]}
Katsottu: 29.4.2020

*Mihalache v. Romania*, Application no. 54012/10 (8.7.2019).
Saatavilla: https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22002-12547%22]}
Katsottu: 29.4.2020

*Rotaru v. Romania*. Application No. 28341/95 (4.5.2000).
Saatavilla: https://hudoc.echr.coe.int/eng#{%22tabview%22:[%22document%22],%22itemid%22:[%22001-58586%22]}
Katsottu: 29.4.2020

*Segersted-Wiberg ja muut v. Ruotsi*. Application no. 62332/00 (6.6.2006) (Final 6.9.2006).
Saatavilla: https://hudoc.echr.coe.int/eng#{"itemid":["001-75591"]}
Katsottu: 29.4.2020

*Z. v. Suomi*. Application no. 22009/93 (25.2.1997).
Saatavilla: https://hudoc.echr.coe.int/eng#{%22tabview%22:[%22document%22],%22itemid%22:[%22001-58033%22]}
Katsottu: 29.4.2020

*Zolotukhin v. Venäjä*. Application no. 14939/03 (7.6.2007) (Final 10.2.2009)
Saatavilla: https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-80962%22]}
Katsottu: 29.4.2020

## Euroopan unionin tuomioistuimen ratkaisut

*Association de médiation sociale (ASM) v. Union Locale des syndicats CGT, Laboudi and others, C-176/12* (15.1.2014).
Saatavilla: http://curia.europa.eu/juris/document/document.jsf?text=&docid=146384&pageIndex=0&doclang=fi&mode=lst&dir=&occ=first&part=1&cid=8303527
Katsottu: 30.4.2020

*Colid McCullough v. Euroopan ammatillisen koulutuksen kehittämiskeskus, C-496/13* (11.6.2015).
Saatavilla: http://curia.europa.eu/juris/document/document.jsf?text=&docid=164964&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=1304832
Katsottu: 29.4.2020

*Digital Rights Ireland Ltd., C-293/12* (6.10.2015).
Saatavilla: http://curia.europa.eu/juris/document/document.jsf?text=&docid=150642&pageIndex=0&doclang=fi&mode=lst&dir=&occ=first&part=1&cid=5585636
Katsottu: 29.4.2020

*Euroopan komissio v. The Bavarian Lager Co. Ltd., C-28/08 P* (29.6.2010).
Saatavilla: http://curia.europa.eu/juris/document/document.jsf?text=&docid=84752&pageIndex=0&doclang=FI&mode=lst&dir=&occ=first&part=1&cid=1304452
Katsottu: 29.4.2020

*František Ryneš v. Úřad pro ochranu osobních údajů, C-212/13* (11.12.2014).
Saatavilla: http://curia.europa.eu/juris/document/document.jsf?text=&docid=160561&pageIndex=0&doclang=FI&mode=lst&dir=&occ=first&part=1&cid=1306042
Katsottu: 29.4.2020

*Google Spain ja Google, C-131/12* (13.5.2014).
Saatavilla: http://curia.europa.eu/juris/document/document.jsf?text=&docid=152065&pageIndex=0&doclang=FI&mode=lst&dir=&occ=first&part=1&cid=1303575
Katsottu: 29.4.2020

*Kärtner Landesregierung, C-594/12* (6.10.2015).
Saatavilla: http://curia.europa.eu/juris/document/document.jsf?text=&docid=150642&pageIndex-=0&doclang=FI&mode=lst&dir=&occ=first&part=1&cid=1302441
Katsottu: 29.4.2020

*Michael Schwarz v. Stadt Bochum, C-291/12* (17.10.2013).
Saatavilla: http://curia.europa.eu/juris/document/document.jsf?text=&docid=143189&pageIndex=0&doclang=FI&mode=lst&dir=&occ=first&part=1&cid=1305507
Katsottu: 29.4.2020

*Rikosoikeudenkäynti v. Bodil Lindqvist, C-101/01* (6.11.2003).
Saatavilla: http://curia.europa.eu/juris/document/document.jsf?text=&docid=48382&pageIndex=0&doclang=FI&mode=lst&dir=&occ=first&part=1&cid=1305235
Katsottu: 29.4.2020

*Scarlet, C-70/10* (24.11.2011).
Saatavilla: http://curia.europa.eu/juris/document/document.jsf?text=&docid=115202&pageIndex=0&doclang=FI&mode=lst&dir=&occ=first&part=1&cid=1305866
Katsottu: 29.4.2020

*Schrems, C-362/14* (6.10.2015).
Saatavilla: http://curia.europa.eu/juris/document/document.jsf?text=&docid=169195&pageIndex=0&doclang=FI&mode=lst&dir=&occ=first&part=1&cid=1304054
Katsottu: 29.4.2020

*Variola v. Amministrazione delle Finanze, C-34/73* (10.10.1973).
Saatavilla: http://curia.europa.eu/juris/showPdf.jsf;jsessionid=8434E191EBF429C0FB77E8222AFA0913?text=&docid=88457&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=7526698
Katsottu: 20.4.2020

**Korkeimman hallinto-oikeuden ratkaisut**

KHO 1996-A-6

KHO 2011:41

KHO 2011:664

KHO 2013:181

KHO 2014:145

KHO 2020:8

**Korkeimman oikeuden ratkaisut**

KKO 1929 II 638

KKO 1997:17

KKO 2001:86

KKO 2010:45

KKO 2010:46

KKO 2013:59

**Tietosuojavaltuutetun ratkaisut**

TSV 17.5.2017: Tietosuojavaltuutetun kannanotto tieteellisen tutkimuksen määritelmästä ja käyttötarkoitussidonnaisuudesta 781/402/17 (Yleistä tietosuoja-asetusta ei vielä tuolloin sovellettu, vaikka se olikin jo voimassaolevaa oikeutta, joten kyseessä ei voinut olla vielä tietosuoja-asetuksen mukainen päätös. Kannanotolla pyrittiinkin ennen kaikkea linjaamaan myöhemmin sovellettavaksi tulevan tietosuoja-asetuksen tulkintaa).

TVS 22.11.2019: Tietosuojavaltuutetun EU:n yleisen tietosuoja-asetuksen mukainen päätös. Rekisteröidyn tunnistaminen ja puheluiden tallentaminen 7713/163/2018.

**Eduskunnan oikeusasiamiehen ratkaisut**

AOA dnro 3447/4/05, (EOAK Dnro 3447/4/05) 10.3.2008. Kyseessä on apulaisoikeusasiamiehen ratkaisu, joten käytän lyhennettä AOA.

**Yhdysvaltain korkeimman oikeuden ratkaisut**

*Goldman v. United States*, 316 U.S. 129 (1942).
Saatavilla: https://supreme.justia.com/cases/federal/us/316/129/
Katsottu: 30.4.2020

*McCulloch v. Maryland*, 17 U.S. (4 Wheat.) 316 (1819).
Saatavilla: https://supreme.justia.com/cases/federal/us/17/316/
Katsottu: 30.4.2020

*Olmstead v. United States*, 277 U.S. 438 (1928).
Saatavilla: https://supreme.justia.com/cases/federal/us/277/438/
Katsottu: 30.4.2020

*Roe v. Wade*, 410 U.S. 133 (1973).
Saatavilla: https://supreme.justia.com/cases/federal/us/410/113/
Katsottu: 30.4.2020

*Silverman v. United States*, 365 U.S. 505 (1961).
Saatavilla: https://supreme.justia.com/cases/federal/us/365/505/
Katsottu: 30.4.2020

*United States v. Hubbell*, 530 U.S. 27 (2000).
Saatavilla: https://supreme.justia.com/cases/federal/us/530/27/
Katsottu: 30.4.2020

*Weems v. United States*, 217 U.S. 349 (1910).
Saatavilla: https://supreme.justia.com/cases/federal/us/217/349/
Katsottu: 30.4.2020

**Yhdysvaltain liittovaltion muutoksenhakutuomioistuinten ratkaisut**

*Balintulo et al. v. Daimler AG et al.* 09-2778-cv(L), August Term, 2009, Decided 21.8.2013 (2013).
Saatavilla: https://cases.justia.com/federal/appellate-courts/ca2/09-2778/09-2778-2013-08-21.pdf?ts=1410918994

*United States v. John Doe*, 670 F.3d 1335, 1337 (11$^{Th}$ Cir. 2012), Grand Jury Subpoena Duces Tecum Dated March 25, 2011 (2012).
Saatavilla: https://stanford.edu/~jmayer/law696/week8/Compelled%20Password%20Disclosure%20(Eleventh%20Circuit).pdf
Katsottu: 30.4.2020

*United States v. Kramer*, 711 F.2d 789, 791 (7$^{th}$ Cir.), cert. denied, 464 U.S. 962 (1983).
Saatavilla: https://casetext.com/case/united-states-v-kramer-3
Katsottu: 30.4.2020

**Yhdysvaltojen osavaltioiden tuomioistuinten ratkaisut**

*Superior Court of New Jersey: VW Credit, Inc. v. Coast Automotive Group, Ltd., et al.* (2002).
Saatavilla: https://law.justia.com/cases/new-jersey/appellate-division-published/2002/a6594-00-opn.html
Katsottu: 30.4.2020

*USDC Southern District of New York: Ntzebesa, et al. v. Citigroup, Inc., et al.* (2014).
Saatavilla: https://law.justia.com/cases/federal/district-courts/new-york/nysdce/1:2002cv04712/37462/170/
Katsottu: 30.4.2020

## Lehdistö

*Gartner, 11.11.2014*. Gartner says 4.9 billion connected "things" will be in use in 2015.
Saatavilla: https://www.gartner.com/newsroom/id/2905717
Katsottu: 29.4.2020

*Helsingin Sanomat, 8.7.2017*. Sijoitusjätti lähetti Suomessa tuhansia kirjeitä, joissa saajan henkilötunnus oli kaikkien nähtävillä.
Saatavilla: https://www.hs.fi/talous/art-2000005284338.html
Katsottu: 29.4.2020

*HR viesti 1/2018*. Digirekry tuli jäädäkseen. Rekrytointi sähköistyy nyt kovaa vauhtia – mutta digitaalisuus ei saa olla itsetarkoitus.

*HR viesti, 1/2018*. GDPR tuo lisätöitä – mutta parantunut tietosuoja on pitkällä tähtäimellä vain hyväksi.

*PR Newswire, 25.1.2018*. ZoomInfo Announces Compliance with the Forthcoming General Data Protection Regulation (GDPR): Ensuring customers and partners are aware of new principles and regulations to better evaluate implications of the GDPR.

*Yrittäjät, 21.2.2017*. EK luopui keskusjärjestösopimuksista – pitääkö ay-jäsenmaksut yhä periä ja tilittää?
Saatavilla: https://www.yrittajat.fi/uutiset/550628-ek-luopui-keskusjarjestosopimuksista-pitaako-ay-jasenmaksut-yha-peria-ja-tilittaa#61ba7629
Katsottu: 29.4.2020

*Yrittäjät, 23.10.2018*. Suomen Yrittäjät: Ay-jäsenmaksujen perimisen ja tilittämisen voi lopettaa.
Saatavilla: https://www.yrittajat.fi/uutiset/598699-sy-ay-jasenmaksujen-perimisen-ja-tilittamisen-voi-lopettaa#61ba7629
Katsottu: 29.4.2020

## Internet-lähteet

*Buttarelli 2017*. Buttarelli, Giovanni. Hitting the ground running: How regulators and businesses can really put data protection accountability into practice. Speech at European Data Protection Days Conferences. EDPS. Berlin 15.5.2017.
Saatavilla: https://edps.europa.eu/sites/edp/files/publication/17-05-15_edpd_keynote_speech_en_0.pdf
Katsottu: 29.4.2020

*Data Protection for Human Rights Defenders, 2018*. Travel Guide to the Digital World: Data Protection for Human Rights Defenders. Global Partners Digital, Lontoo 2018.
Saatavilla: https://www.gp-digital.org/wp-content/uploads/2018/07/travelguidetodataprotection.pdf
Katsottu: 29.4.2020

*Euroopan komissio: Mitä tarkoittaa 'sisäänrakennettu' ja 'oletusarvoinen' tietosuoja?*
Saatavilla: https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/what-does-data-protection-design-and-default-mean_fi
Katsottu: 29.4.2020

*Euroopan komission tiedote, 12.6.2016*. European Commission – Press release: from European Commission launches EU-U.S. Privacy Shield: stronger protection for transatlantic data flows.
Saatavilla: https://ec.europa.eu/commission/presscorner/detail/en/IP_16_2461
Katsottu: 29.4.2020

*European Data Protection Supervisor, 7.6.2016*. EPDS, Accountability factsheet 7.6.2016.
Saatavilla: https://edps.europa.eu/sites/edp/files/publication/16-06-07_accountability_factsheet_en.pdf
Katsottu: 29.4.2020

*ICO:n ohje: Principle (f): Integrity and confidentiality (security)*. Information Commissioner's Office (ICO, Ison-Briannian tietosuojaviranomainen), ohje: Guide to the General Data Protection Regulation (GDPR): Principle (f): integrity and confidentiality (security).
Saatavilla: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/integrity-and-confidentiality-security/
Katsottu: 29.4.2020

*ICO:n ohje: Security*. Information Commissioner's Office (ICO, Ison-Britannian tietosuojaviranomainen), ohje: Guide to the General Data Protection Regulation (GDPR): Security.
Saatavilla: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/security/
Katsottu: 29.4.2020

*Information Commissioner's Office (ICO, Ison-Britannian tietosuojaviranomainen), ohje: Principle (d): Accuracy*. Guide to the General Data Protection Regulation (GDPR).
Saatavilla: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/accuracy/
Katsottu: 29.4.2020

*Oikeusministeriön tiedote, 1.3.2018*. Oikeusministeriö: Tietosuojalaki täydentäisi EU:n tietosuoja-asetusta. Tiedote 1.3.2018.
Saatavissa: http://oikeusministerio.fi/artikkeli/-/asset_publisher/tietosuojalaki-taydentaisi-eu-n-tietosuoja-asetusta
Katsottu: 29.4.2020

*TEM:n opas, 4/2017*. TEM oppaat ja muut julkaisut, 4/2017. Uuden hankintalainsäädännön velvoitteet rikosrekisteriotteiden selvittämisestä, antanut työ- ja elinkeinoministeriö 2017.
Saatavilla: http://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/79882/TEM_oppaat_4_2017_Uuden_hankintalainsaadannon_velvoitteet_08052017.pdf
Katsottu: 29.4.2020

*Tietosuojavaltuutetun toimisto, 26.9.2013*. Tietosuojavaltuutetun toimisto: Henkilötietolain taustaa, julkaisu 26.9.2013.
Satavilla: http://www.tietosuoja.fi/fi/index/rekisterinpitajalle/henkilotietolaintaustaa.html
Katsottu: 29.4.2020

*Tietosuojavaltuutetun toimiston ohje: Arvioi riskit ja suunnittele toimenpiteet tietosuojan toteuttamiseksi*.
Saatavilla: https://tietosuoja.fi/arvioi-riskit
Katsottu: 29.4.2020

*Tietosuojavaltuutetun toimiston ohje: Automaattinen päätöksenteko ja profilointi*.
Saatavilla: https://tietosuoja.fi/automaattinen-paatoksenteko-profilointi
Katsottu: 29.4.2020

*Tietosuojavaltuutetun toimiston ohje: Osoita noudattavasi tietosuojalainsäädäntöä*.
Saatavilla: https://tietosuoja.fi/osoitusvelvollisuus
Katsottu: 29.4.2020

*Tietosuojavaltuutetun toimiston ohje: Rekisteröidyn oikeuksista poikkeaminen tieteellisen tai historiallisen tutkimuksen tai tilastoinnin yhteydessä*.
Saatavilla: https://tietosuoja.fi/rekisteroidyn-oikeuksista-poikkeaminen
Katsottu: 29.4.2020

*Tietosuojavaltuutetun toimiston ohje: Yritystä koskevat sitovat säännöt*.
Saatavilla: https://tietosuoja.fi/yritysta-koskevat-sitovat-saannot
Katsottu: 29.4.2020

*Tietosuojavaltuutetun toimiston tiedote, 1.3.2018*. Tietosuojavaltuutetulle uusia tehtäviä ja toimivaltuuksia.
Saatavilla: http://www.tietosuoja.fi/fi/index/ajankohtaista/tiedotteet/on/03/tietosuojavaltuutetulleuusiatehtaviajatoimivaltuuksia.html
Katsottu: 29.4.2020

**Internet-sivustot**

Euroopan komission ylläpitämä sivusto, jossa on tietoa yleisestä tietosuoja-asetuksesta (Data Protection Reform, Factsheets).
Saatavilla: http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=52404
Katsottu: 29.4.2020

Euroopan neuvoston (EN) ylläpitämä sivusto, joka sisältää useita tietosuojaan liittyviä suosituksia.
Saatavilla: https://www.coe.int/en/web/cdcj/recommendations-resolutions-guidelines
Katsottu: 29.4.2020

Euroopan tietosuojaneuvoston (EDPB, engl. European Data Protection Board) kotisivut. Euroopan tietosuojaneuvosto on riippumaton unionin elin, joka koostuu EU:n kansallisista tietosuojaviranomaisista ja Euroopan tietosuojavaltuutetun edustajista. Myös ETA-maat Islanti, Norja ja Liechtenstein ovat tietosuojaneuvoston jäseniä. Euroopan tietosuojaneuvosto vastaa EU:n yleisen tietosuoja-asetuksen sekä poliisi- ja rikosoikeusviranomaisia koskevan tietosuojadirektiivin yhdenmukaisesta soveltamisesta.
Saatavilla: https://edpb.europa.eu/edpb_fi
Katsottu: 29.4.2020

Euroopan tietosuojavaltuutetun (EDPS, engl. European Data Protection Supervisor) kotisivut.
Saatavilla: https://edps.europa.eu/
Katsottu: 2.5.2020

Privavy Shield -sopimuksen johdosta luodut nettisivut (The EU-U.S. and Swiss-U.S. Privacy Shield Framework by the U.S. Department of Commerce and the European Commission and Swiss Administration). Tämän sivuston kautta on saatavissa tietoa Privacy Shield -järjestelystä sekä tarkastettavissa, onko tietty yhtiö rekisteröity Privacy Shieldin puitteissa hyväksytyksi toimijaksi ja näin ollen, onko toimijalle oikeutettua siirtää henkilötietoja EU/ETA:n tai Sveitsin sisältä Yhdysvaltoihin.
Saatavilla: https://www.privacyshield.gov/welcome
Katsottu: 2.5.2020

Suomen tietosuojavaltuutetun toimiston ohjeistuksia ja lomakkeita sisältävä kotisivu.
Saatavilla: https://tietosuoja.fi/etusivu
Katsottu: 29.4.2020

Suomen valtiovarainministeriön kotisivut, jotka sisältävät useita tietosuojaa sekä tarkemmin osoitusvelvollisuutta koskevia ohjeita, kuten tietosuojan osoitusvelvollisuutta edistävien työpajatilaisuuksien koulutusmateriaalit.
Saatavilla: https://vm.fi/haku/-/q/osoitusvelvollisuus
Katsottu: 29.4.2020

Tietosuojatyöryhmän (WP-29, engl. Article 29 Data Protection Working Party) kotisivut.
Saatavilla: http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083
Katsottu: 29.4.2020

# I. JOHDANTO

## 1. Aluksi

Toukokuun 25. päivänä 2018 on tullut Euroopan unionin (EU) jäsenvaltioissa suoraan sovellettavaksi yleinen tietosuoja-asetus (EU) 679/2016, josta käytetään myös lyhennettä GDPR (engl. *General Data Protection Regulation*). Koska kyseessä on asetus, ei sen soveltaminen edellytä lainsäädäntötoimia jäsenvaltioilta. Yleisen tietosuoja-asetuksen päätavoitteena on yhdenmukaistaa[1] jäsenvaltioiden tietosuojalainsäädäntöä ja helpottaa palveluiden rajat ylittävää tarjontaa.

Tietosuoja-asetus tuo uusia henkilötietojen käsittelyä koskevia velvoitteita. Lisäksi asetuksessa säädetään rekisteröityjen uusista oikeuksista, jotka rekisterinpitäjän sekä henkilötietojen käsittelijän tulee huomioida noudattaakseen asetusta. Tietosuoja-asetus antaa rekisteröidyille myös mahdollisuuden hakea vahingonkorvausta valintansa mukaan joko henkilötietojen käsittelijältä, rekisterinpitäjältä tai keneltä tahansa käsittelyyn osallistuneelta yhteisrekisterinpitäjältä. Edellä mainittu on johtanut muun muassa siihen, että monet ennen yleisen tietosuoja-asetuksen voimaantuloa solmitut henkilötietojen käsittelyä koskevat sopimukset, joilla tyypillisesti henkilötietojen käsittelijät ovat pyrkineet rajaamaan vastuutaan, ovatkin pätemättömiä 25.5.2018 lähtien, sillä tietosuoja-asetus on pääosin pakottavaa lainsäädäntöä, eikä sen sisällöstä näin ollen voi sopimuksin poiketa. Tämä on puolestaan johtanut tarpeeseen neuvotella useimmat henkilötietojen käsittelyä koskevat sopimukset uudelleen.

Vanhastaan on vallinnut välinpitämättömyys tietosuojavelvoitteita kohtaan, minkä takia tietosuoja-asetuksen voimaan tullessa monissa yhtiöissä ja organisaatioissa tietosuojakäytännöt eivät täyttäneet edes vanhan henkilörekisterilain (471/1987) tai sen kumonneen henkilötietolain (523/1999) asettamia vaatimuksia. Juuri edellä mainitusta välinpitämättömyydestä johtuen uusi tietosuoja-asetus mahdollistaakin hallintopakon käyttämisen eli tietosuojaviranomainen voi määrätä tuntuvia hallinnollisia sakkoja sekä rekisterinpitäjälle että henkilötietojen käsittelijälle, joka ei noudata yleisen tietosuoja-asetuksen mukaisia velvoitteita. Asianajaja Mari Rusi onkin todennut vuonna 2018, että suurilla organisaatioilla on laajalti käynnissä projekteja, joilla pyritään ohjaamaan tietosuojakäytännöt GDPR-yhteensopiviksi. Hänen mukaansa keskeisin osa näitä tietosuojaprojekteja on osoitusvelvollisuus, joka pitää sisällään nykytilan kartoituksen sekä tietosuojan huomioimisen osana toimintojen suunnittelua ja mallinnusta.[2] Osoitusvelvollisuus johtaa käytännössä siihen, että kaikkien tietosuojaperiaatteiden toteutus tulee kyetä osoittamaan prosesseja ja menettelytapoja sekä käytännön toteutusta koskevan tarkan dokumentoinnin avulla. Tietosuojaviranomaisella puolestaan

[1] Ks. esim. Voutilainen et al. 2013, s. 372.

[2] HR viesti 1/2018, huomaa myös: ”*EU:n yleinen tietosuoja-asetus muuttaa maailmaa ja tuo mukanaan entistä tiukempia tietosuojavaatimuksia. Vaatimusten noudattamatta jättämisestä voi seurata tuntuvia sakkoja, jotka voivat nousta jopa 20 miljoonaan euroon tai 4 prosenttiin yrityksen liikevaihdosta. - - Yrityksen on mietittävä tarkkaan, kuka tietoa käsittelee, miksi ja kauanko tietoa säilytetään.*”

on oikeus saada nähtävilleen tämä dokumentaatio, varmistaakseen osoitusvelvollisuuden noudattamisen.

## 2. Tutkielman tausta ja aihe

Globalisaatio sekä toisaalta työvoiman, pääoman, tavaroiden ja palveluiden vapaa liikkuvuus Euroopan unionissa ovat johtaneet tarpeeseen säännellä yhä tarkemmin myös henkilötietojen käsittelyä.[3] Edeltävä kansallinen tietosuojalainsäädäntömme perustui Euroopan parlamentin ja neuvoston yksilöiden suojelusta henkilötietojen käsittelyssä ja näiden tietojen vapaasta liikkuvuudesta annettuun direktiiviin 95/46/EY (*henkilötietodirektiivi*). Ongelmalliseksi on kuitenkin muodostunut se, että direktiivi on mahdollistanut sen, että EU:n jäsenvaltioilla on ollut 28 erilaista tietosuojaa koskevaa lainsäädäntöä.[4] Pakottavana instrumenttina[5] yleinen tietosuoja-asetus yhtenäistää entisestään tietosuojalainsäädäntöä EU:n sisällä sekä niitä velvoitteita, joiden täyttyessä henkilötietoja voi luovuttaa kolmansiin valtioihin. Tietosuojakäytäntöjen yhtenäistämisen katsotaan johtavan kansalaisten entistä parempaan luottamukseen siitä, että heidän henkilötietojensa käsittely tapahtuu asianmukaisesti. Yleinen tietosuoja-asetus ei kuitenkaan juurikaan muuta henkilötietojen käsittelyn perusperiaatteita.[6]

Edeltänyt henkilötietolaki on jo kumottu ja sen tilalle on säädetty tietosuojalaki (1050/2018), jonka on ollut tarkoitus hallituksen esityksen mukaan tulla voimaan 25.5.2018. Kyseisestä ajankohdasta kuitenkin myöhästyttiin Suomessa. Lainsäätämisvaiheessa todettiin, että uuden tietosuojalain on oltava sisällöltään yleisen tietosuoja-asetuksen mukainen ja siitä poikkeaminen on mahdollista ainoastaan niissä kohdin, joissa asetus mahdollistaa tällaisen liikkumavaran (engl. *leeway*) käytön. On myös syytä korostaa, että yleinen tietosuoja-asetus koskee kaikkia yhtiöitä, niiden koosta riippumatta. Koska jokaisessa yrityksessä käsitellään henkilötietoja toimialasta riippumatta, muun muassa työoikeudellisten velvoitteiden takia, ei tietosuoja-asetuksen asettamilta vaatimuksilta voi täysin välttyä. Käytännössä yhdenkin asiakkaan tai työntekijän tietojen käsittely johtaa yleisen tietosuoja-asetuksen soveltamiseen.[7]

Yleisen tietosuoja-asetuksen mukaan ”*luonnollisten henkilöiden suojelu henkilötietojen käsittelyn yhteydessä on perusoikeus*”. Lisäksi todetaan, että ”*jokaisella on oikeus henkilötietojensa suojaan*”. Tämä on yhdenmukaista perustuslakimme (PL, 731/1999) 10 §:n 1 momentin kanssa, jonka mukaan

[3] Ks. Tarkela 2016, s. 78.
[4] Kremer 2016, s. 136.
[5] Craig et al. 2015, s. 87 ja 105—122 sekä erityisesti asetuksista s. 107: Eurooppaoikeudellisten instrumenttien hierarkiasta ja suorasta vaikutuksesta sekä sovellettavuudesta. Asetus on oikeudellisena instrumenttina primaarilähteistä perustansa saava suoran vaikutuksen omaava ja suoraan sovellettava oikeuslähde. Yleinen tietosuoja-asetus on nimensä mukaisesti asetus. Primaarilähteitä ovat puolestaan unionin perussopimukset, ja niihin perustuvia sekundaarilähteitä ovat esimerkiksi asetukset ja direktiivit.
[6] Oikeusministeriön tiedote, 1.3.2018.
[7] Ks. esim. Hoikka et al. 2017, s. 15.

”*jokaisen yksityiselämä, kunnia ja kotirauha on turvattu. Henkilötietojen suojasta säädetään tarkemmin lailla*.” Perustuslaki asettaa siis vaatimukseksi säätää laintasoisesti tarkemmin tietosuojasta. Näin ollen oikeusministeriö asetti helmikuussa 2016 työryhmän valmistelemaan lainsäädäntöehdotusta, jolla täytettiin yleisen tietosuoja-asetuksen vaatimukset sekä asetuksen asettamat mahdollisuudet kansallisen liikkumavaran käytölle.[8]

Yleisen tietosuoja-asetuksen 83 artiklassa säädetään hallinnollisista sakoista, joita tietosuojaviranomaisen on mahdollista määrätä, mikäli tietosuoja-asetuksen määräämiä tietosuojavelvoitteita rikotaan. Nämä hallinnolliset sanktiot toimivat yleisestävästi pelotteina, jotta rekisterinpitäjät ja henkilötietojen käsittelijät suhtautuisivat riittävällä vakavuudella ja tarkkuudella yksilöiden yksityisyyden suojaa turvaaviin tietosuojavelvoitteisiin. Esimerkiksi Sponda Oyj on lähettänyt osakkeenomistajilleen kirjekuoria, joista ilmeni jo päältäpäin osakkeenomistajien henkilötunnukset.[9] Näiden ”inhimillisten” virheiden määrä todennäköisesti vähenee hallinnollisten sanktioiden aikaansaaman pelotteen myötä, kun tietosuojavelvoitteiden rikkomisesta voi jatkossa seurata konkreettisia taloudellisesti suuriakin sanktioita.

Tutkielmani aiheena on rekisterinpitäjän osoitusvelvollisuus (*accountability*) ja tutkimuskysymykseni mukaisesti selvitettäväksi tulevat rekisterinpitäjälle osoitusvelvollisuuden nojalla kohdentuvat toimintavelvoitteet. Osoitusvelvollisuudesta säädetään tietosuoja-asetuksen 5 artiklan 2 kohdassa, jonka mukaan rekisterinpitäjän tulee pystyä osoittamaan toimintansa täyttävän asetuksen mukaiset tietosuojavelvoitteet ja erityisesti rekisteröityjen oikeudet.[10] Havainnollistavana esimerkkinä digitalisoitumisen luomien mahdollisuuksien aiheuttamista riskeistä, jotka osoittavat osoitusvelvollisuuden tarpeellisuuden, voidaan mainita muun muassa se, että nykyisin kokeillaan jo sosiaaliseen mediaan integroituvia rekrytointijärjestelmiä, jotka luovat suoran väylän yritysten ja työnhakijoiden välille.[11] Tällaisten järjestelmien käyttäminen on kuitenkin erityisen riskialtista tietosuojan kannalta, sillä uudet tekniikat mahdollistavat työnhakijoiden profiloimisessa myös sellaisten tietojen automatisoidun käsittelyn, mitä ei tulisi sisällyttää valintaperusteisiin. Osoitusvelvollisuuden nojalla rekisterinpitäjän tuleekin osoittaa, että uusi teknologia uusine ominaisuuksineen, ei johda tietosuojaperiaatteiden vastaisiin mekanismeihin ja käytäntöihin.

Osoitusvelvollisuuden tarpeellisuuden tuo esille myös teknologisen kehityksen mahdollistamat uudet kerätyn datan käyttömuodot. Kun nykyisin voidaan jo puhua ubiikkiyhteiskunnasta, jolla tarkoitetaan sitä, että yhteiskunnassa tietojenkäsittelyjärjestelmät ovat hajautettu sekä hyödynnettävissä olevat tiedot ovat laajalti yhteiskunnan eri osa-alueilla, niin ubiikkiin tietoympäristöön liittyy

[8] TATTI-mietintö 35/2017, s. 13.
[9] Helsingin Sanomat, 8.7.2017.
[10] Ks. esim. Kremer 2016, s. 138.
[11] HR viesti 1/2018.

keskeisenä ominaisuutena myös mahdollisuus yhdistellä kerättyä tietoa muuhun aikaisemmin kerättyyn tietoon.[12] Tällöin rekisteröidyn voi olla hyvin hankala havaita, antamansa henkilötietojen käsittelemiseksi yleensä vaadittavan suostumuksen merkitystä. Näiden internettiin kytkeytyvien, ubiikkiyhteiskunnalle tyypillisten, laitteiden määrän arvioidaan kohoavan vuoden 2020 aikana jopa 25 miljardiin.[13] Nykyisellä massadatan aikakaudella tietojen arvo ei perustukaan enää pelkästään niiden alkuperäiseen käyttötarkoitukseen, vaan datan arvoon vaikuttaa vahvasti myös niiden uudet käyttömahdollisuudet.[14]

Vuonna 2013 tapahtunut NSA-skandaali on muuttanut huomattavasti henkilötietojen turvallisen käsittelyn merkitystä sekä kansainvälisellä että kansallisella tasolla. Myös tämä on lisännyt painetta muuttaa sääntelyä yksityiskohtaisemmaksi ja luoda yksilöille entistä paremmat puitteet hallita itseään koskevia tietoja. Yksityiskohtaisempaan sääntelyyn sysännyttä painetta on varmasti lisännyt myös se, että noin 80 prosenttia internetin käyttäjistä suhtautuu kielteisesti häntä koskevien tietojen taloudelliseen hyödyntämiseen. Yhä useammat kokevat, ettei heillä ole mahdollisuutta vaikuttaa omien tietojensa muiden toimesta tapahtuvaan taloudelliseen hyödyntämiseen.[15]

## 3. Tutkielman tavoite, rakenne ja rajaus

Henkilötietodirektiivi on tullut voimaan vuonna 1995, jolloin tietojärjestelmät sekä tekninen toimintaympäristömme olivat hyvin erilaisia kuin nykypäivänä. Henkilötietodirektiivi saatettiin voimaan jokaisessa EU:n jäsenvaltiossa kansallisella lailla, mikä on johtanut siihen, että tietosuojasääntelyn sisältö on voinut voimakkaastikin vaihdella eri jäsenvaltioiden välillä. Tämä on johtanut siihen, että esimerkiksi monikansallisten yritysten on ollut monimutkaista noudattaa tietosuojalainsäädäntöä, kun eri jäsenvaltioissa on erilaiset käytännöt esimerkiksi ilmoitusvelvollisuuden täyttämiseksi paikalliselle tietosuojaviranomaiselle. Muun muassa näistä syistä EU:ssa ryhdyttiin säätämään jo 14.4.2016 valmistunutta ja 24.5.2016 voimaan tullutta EU:n yleistä tietosuoja-asetusta, joka kumosi henkilötietodirektiivin ja jonka soveltaminen alkoi 25.5.2018.[16] Voimaantulon ja soveltamisen alkamisen välistä aikaa kutsutaan siirtymäajaksi, jolloin yhtiöt pyrkivät saamaan tietosuojakäytäntönsä suoraan sovellettavan asetuksen mukaisiksi.[17] Tutkielmani rajautuu nimenomaan yleisen tietosuoja-asetuksen hahmottamiseen rekisterinpitäjän näkökulmasta, joten kansallinen lainsäädäntö ei ole yhtä keskeisessä osassa tutkielmaani.

[12] Karhula 2008, s. 11—12.
[13] Gartner, 11.11.2014. Tällöin internettiin kytkeytyvien laitteiden määrä on viisinkertaistunut viimeisimmän viiden vuoden aikana.
[14] Kallasvuo 2016, s. 141—142.
[15] Ks. esim. Kallasvuo 2016, s. 143 ja s. 158.
[16] Pitkänen et al. 2017, s. 1.
[17] Ks. esim. PR Newswire, 25.1.2018.

Tutkielman tavoitesivumäärä asettaa omat haasteensa, minkä takia maisteritutkielmani on rajattu koskemaan nimenomaan yleisessä tietosuoja-asetuksessa säädetyn osoitusvelvollisuuden vaikutusta rekisterinpitäjän toimintaan yleisesti, ja erityisesti, kun rekisterinpitäjä ulkoistaa henkilötietojen käsittelyä kolmansille osapuolille. Tässä yhteydessä ei siis tulla kattavasti vertailemaan tietosuoja-asetuksen sisältöä suhteessa edeltäneeseen henkilötietodirektiiviin. Edellä mainitun asiakysymyksen lisäksi tulen tutkimaan sitä, millä tavoin rekisterinpitäjän on osoitusvelvollisuuden puitteissa osoitettava noudattavansa tietosuojalainsäädäntöä toimivaltaiselle tietosuojaviranomaiselle. Tällöin esille nousevat viranomaisen ennakko- ja jälkivalvontakeinot, joiden puitteissa osoitusvelvollisuuden täyttäminen lopulta arvioidaan. Myös ulkoistustilanteissa tämä vastuu on ulkoistetun käsittelytoiminnan osaltakin rekisterinpitäjällä.

Tutkielmani alussa, johdanto-osan jälkeisessä toisessa osassa, tuon esille perus- ja ihmisoikeusnäkökulmaa liittyen henkilötietojen suojaan. Koen tämän tärkeäksi, sillä monesti tietosuojavelvoitteet nähdään organisaation sisällä ainoastaan rasitteina, joiden toteuttaminen vaatii hallinnollisia resursseja. Usein unohdetaankin, että tietosuojavelvoitteilla nimenomaisesti suojataan luonnollisten henkilöiden perus- ja ihmisoikeuksia ja erityisesti oikeutta henkilötietojen suojaan sekä yksityisyyteen. Toisen osan tarkoituksena on tuoda esille, miksi osoitusvelvollisuuden säätäminen on ollut tarpeellista ja toisaalta perusoikeusmyönteisen laintulkinnan vaatimuksesta johtuen, millä tavalla osoitusvelvollisuutta ja muutakin tietosuojalainsäädäntöä tulee tulkita.

Kolmannessa osassa pyrin selvittämään, mitä osoitusvelvollisuudella yleisellä tasolla tarkoitetaan ja millaisia toimia osoitusvelvollisuuden toteuttaminen edellyttää rekisterinpitäjän organisaatiossa. Tarkoitus olisi myös systematisoida osoitusvelvollisuus muiden tietosuojaperiaatteiden joukkoon. Oikeusperiaatteet ovat pohjimmiltaan optimointikäskyjä, jolloin arvioitavaksi tulee myös se, ovatko jotkin tietosuojaperiaatteet mahdollisesti vastakkaisia osoitusvelvollisuuden kanssa ja toisaalta, voivatko jotkin oikeusperiaatteet syrjäyttää osoitusvelvollisuuden[18]. Koska osoitusvelvollisuuden täyttymisen arvioi lopulta tietosuojaviranomainen, tulen kolmannessa osassa ottamaan kantaa valvontaviranomaisen ennakkovalvonta- ja jälkivalvontakeinoihin.

Maisteritutkielmani aiheena on osoitusvelvollisuuden vaikutukset konsernin toimintaan ja erikseen myös niihin tilanteisiin, kun rekisterinpitäjä ulkoistaa henkilötietojen käsittelyn toiselle yhteisölle eli henkilötietojen käsittelijälle. Olen systematisoinut osoitusvelvollisuuden käytännön toteuttamisen siis kahteen osaan, eli kolmannessa osassa kuvattuihin tilanteisiin, joissa on kyse rekisterinpi-

[18] Huomaa, että tutkielmani perusteella esimerkiksi sananvapaus saattaa syrjäyttää tietyiltä osin tietosuojan, joka johtaa siihen, ettei osoitusvelvollisuutta noudateta täysimääräisesti esimerkiksi journalistisessa toiminnassa.

täjän omasta käsittelytoiminnasta, sekä tilanteisiin, joissa on kyse ulkoistetusta rekisterinpitäjän lukuun tapahtuvasta käsittelytoiminnasta. Jälkimmäisiä tapauksia koskee GDPR:n kattavat erityissäännökset.

Näin ollen, tutkielman neljännessä osassa pyrin nostamaan esille nimenomaan niitä osoitusvelvollisuuden noudattamisesta johtuvia toimia, jotka konkretisoituvat ulkoistustilanteissa. Toisin sanoen vastaan kysymykseen, mitä rekisterinpitäjän tulee osoitusvelvollisuuden nojalla tehdä, jotta tämä voi ulkoistaa henkilötietojen käsittelyn. Kysymys on tutkielmani yleisestä tutkimuskysymyksestä, eli siitä mitä organisaation tulisi tehdä pystyäkseen osoittamaan tietosuojaviranomaiselle noudattavansa osoitusvelvollisuutta, johdettu tutkimuskysymys. Maisteritutkielmani tavoitteena on siis konstruoida rekisterinpitäjälle yleisestä tietosuoja-asetuksesta osoitusvelvollisuuden nojalla johtuvat toimintavelvoitteet, jotka tulevat lopulta arvioiduiksi viranomaisen ennakko- ja jälkivalvonnassa.

## 4. Tutkielman menetelmä

Oikeustieteen tarkoituksena on muun muassa oikeusjärjestyksen systematisointi sekä tulkinta ja toisaalta voimassaolevan oikeuden sisällön esittäminen hyödyntäen oikeuslähdeoppien rakenteita.[19] Oikeustiede on yläkäsite, joka voidaan jakaa useampiin osa-alueisiin. Lainoppi eli oikeusdogmatiikka on yksi näistä oikeustieteen haaroista[20] ja tulen käyttämään sitä tutkielmani menetelmänä.

Lainopilla tarkoitetaan voimassa olevien oikeusnormien tulkitsemista ja systematisointia sekä oikeusperiaatteiden, joita oikeusnormit ilmentävät, punnintaa ja yhteensovittamista, tavoitteena luoda rationaalisia suosituksia perustelluiksi oikeudellisiksi tulkintaratkaisuiksi.[21] Oikeusdogmaattinen tutkimus keskittyy toisinaan lokeroimaan oikeusjärjestystä yhä pienempiin kokonaisuuksiin ja toteuttaa näiden pienten lokeroiden sisällä lainopillista tulkintaa. Tämä johtaa siihen, että oikeudellisten ongelmien ratkaiseminen tai jopa tunnistaminen oikeudenalat ylittäen, muodostuu hankalaksi puhtaasti oikeusdogmaattisilla menetelmillä.[22] Edellä mainittujen ongelmien välttämiseksi olisi mielestäni perustellumpaa käyttää oikeudenalan rajat ylittävää tutkimuksellista otetta, jota kutsutaan ongelmakeskeiseksi lainopiksi[23]. Tutkielmassani pyrinkin tuomaan esille osoitusvelvollisuuden vaikutusta sopimuskäytäntöön ja vahingonkorvaus- sekä hallinto-oikeuteen.

Kuten todettu, oikeusdogmatiikassa keskitytään voimassaolevan oikeuden tulkitsemiseen ja systematisointiin. On syytä huomata, että yleinen tietosuoja-asetus on ollut voimassa olevaa oikeutta jo noin neljä vuotta, vaikkei sitä vielä olekaan sovellettu kuin kahden vuoden ajan. Kansallisen lainsäädännön osalta olen joutunut käyttämään velvoittavien oikeuslähteiden lisäksi aineistona lähinnä

[19] Voutilainen 2009, s. 9.
[20] Nuotio 2005, s. 130—131.
[21] Aarnio 1999, s. 332.
[22] Wallin 2002, s. 144.
[23] Voutilainen 2009, s. 11.

tietosuojalain esitöitä, sillä kyseisen lain soveltamisesta on olemassa vielä hyvin vähän oikeuskäytäntöä. Mietinnöt ja lausunnot sekä hallituksen esitys antavat kuitenkin, yhdessä tietosuoja-asetuksen kanssa, hyvän pohjan tutkimusongelmani ratkaisemiseksi. Vaikka yleiseen tietosuoja-asetukseen pohjautuvaa kansallista lainsäädäntöä säädetään edelleen tiettyjen erityislakien muodossa, niin joka tapauksessa tulevan kansallisen tietosuojalainsäädännön tulee olla, jo hyvinkin yksityiskohtaista sääntelyä sisältävän, tietosuoja-asetuksen mukaista.

On myös huomattava, että tietosuoja-asetus ei aseta juurikaan muutoksia jo henkilötietodirektiivin aikana vallinneeseen tietosuojaoikeuteen, erityisesti tietosuojaperiaatteiden tasolla. Näin ollen pidän myös perusteltuna käsitellä ja tulkita jonkin verran aikaisempaa oikeuskäytäntöä, kuitenkin lähinnä siltä osin, kun kyse on sellaisista tietosuojaperiaatteista, jotka velvoittivat rekisterinpitäjiä ja henkilötietojen käsittelijöitä jo henkilötietodirektiivin aikakaudella. Mielestäni aikaisemman oikeuskäytännön pohjalta voi joiltain osin perustellusti tehdä analogisia päätelmiä, vaikka sovellettava lainsäädäntö muuttuikin.

Tutkielmani aihe sopisi hyvin oikeusinformatiikan oikeudenalaan kuuluvaksi tutkimukseksi, mutta tietosuojaoikeutta on perusteltua tarkastella myös hallinto-oikeudellisesta näkökulmasta. Tulenkin tutkimuksessani tulkitsemaan tietosuojaperiaatteita hallinto-oikeudellisia perusperiaatteita vasten, sillä oikeusinformatiikka on kehittynyt informaatio-oikeudesta eriytymällä omaksi oikeudenalakseen. Informaatio-oikeudessa, jota on käytetty jopa synonyyminä oikeusinformatiikalle, on puolestaan ollut kyse erityishallinto-oikeudesta, josta on ajan saatossa muodostunut oma oikeudenalansa.[24] On myös huomattava, että kaikista tietosuojaviranomaisen päätöksistä haetaan muutosta hallinto-oikeuksista, mikäli oikeudenalajaotusta halutaan tarkastella tuomioistuinlinjojen näkökulmasta. Käytännössä nimenomaan osoitusvelvollisuuden täyttymisen arvioijana tietosuojaviranomaisella, hallinto-oikeuksien ja korkeimman hallinto-oikeuden (KHO) ohella, on tässä suhteessa tulkintamonopoli.[25]

[24] Koivisto 2015, s. 969; ks. myös esim. Mäenpää 2013, s. 46.

[25] Ks. Niemi 2015, s. 337—338, jonka mukaisesti hallintoprosessin kohde on selkeä erottava tekijä yksityis- ja julkisoikeuden välillä. Osoitusvelvollisuuden täyttämiseen liittyvät valitukset kuuluvat hallinto-oikeuden alaan, sillä kyse on viranomaisen tekemästä hallintopäätöksestä, jossa kiista muodostuu yksityisen ja julkisen väliselle vertikaalisuhteelle; s. 334, Toisaalta Johanna Niemi toteaa yksityis- ja julkisoikeudesta, että tätä rajanvetoa on pidetty joskus myös osin keinotekoisena; ks. myös oikeudenalajaotuksen keinotekoisuudesta Wilhelmsson 2000, s. 33; Huomaa lisäksi Halila 2016, s. 292, jossa todetaan hallintoprosessin kuuluvan hallinto-oikeuden alaan. Leena Halila toteaa tämän olevan jopa hiukan valitettavaa, sillä näin kyseinen prosessilaji on jäänyt jokseenkin *”vieraaksi laajasti ymmärretyn prosessioikeuden kentässä”*.

# II. HENKILÖTIETOJEN SUOJA KANSAINVÄLISTEN JA EUROOPPALAISTEN PERUS- JA IHMISOIKEUKSIEN NÄKÖKULMASTA

## 1. Tietosuojan historia

Yksilön kunnioittamista voidaan pitää henkilö- ja persoonallisuusoikeudellisena perusperiaatteena. Yksityisyyden voidaan nähdä historiallisessa katsannossa juontavan juurensa yksilön kunnioittamiseen liittyvästä itsemääräämisoikeudesta. Sittemmin yksityisyyden voidaan katsoa erottuneen omaksi erilliseksi käsitteeksi yksilön itsemääräämisoikeudesta.[26] Laajentavasti tulkiten yksilön itsemääräämisoikeus tarkoittaa luonnollisen henkilön oikeutta valvoa oikeuksiensa toteutumista ja toisaalta oikeutta päättää itseään koskevista asioista, mukaan lukien omien henkilötietojensa käsittelystä.[27] Itsemääräämisoikeuden keskeistä perusoikeudellista asemaa ilmentää perustuslain 1 §:n maininta yksilön oikeuksien ja vapauksien turvaamisesta.[28] Näin ollen tutkittaessa henkilötietojen suojaa koskevaa oikeudellista kehittymistä omaksi eksplisiittiseksi perusoikeudekseen, on luontevinta lähestyä asiaa itsemääräämisoikeuden ja yksityisyyden käsitteen näkökulmasta. Toisaalta myös julkisuusperiaatetta on aiheellista käydä läpi yksityisyyden vastinparina.

### 1.1. Yksityisyys

Yksityisyys on nähty alkujaan yhtenä itsemääräämisoikeuden elementtinä persoonallisuusoikeudellisessa käsitteistössä. Yksityisyyden (*privacy*) käsitteen oikeustieteelliset juuret sijoittuvat Yhdysvaltoihin.[29] Suomalaisessa lakitekstissä yksityisyyden käsite omaksuttiin henkilörekisterilain myötä vuonna 1987. Yhdysvaltalaisessa oikeustieteessä puolestaan yksityisyyden ytimeksi oli jo muotoutunut yksilön oikeus kontrolloida itseään koskevien tietojen käsittelyä sekä oikeus olla rauhassa suhteessa laajempaan yleisöön.[30] Alkujaan yksityisyyden käsite ei kuitenkaan sisältynyt Yhdysvaltain perustuslakiin, vaan käsite on kehittynyt sitovaksi oikeudelliseksi periaatteeksi oikeuskäytännön nojalla.[31] Kun arvioidaan yksityisyyden luonnetta perus- ja ihmisoikeutena, on syytä huomioida, että eksplisiittisten ja implisiittisten perusoikeuksien konstruoimisessa on kyse vallan käytön ytimessä olevien normien määrittelystä.[32]

Suomessa yksityisyyttä oikeudellisena käsitteenä alettiin tutkia hallinto- ja henkilöoikeudellisesta näkökulmasta valtiosääntöoikeudellista taustaa vasten. Globaalilla tasolla yksityisyyden käsitteen

---

[26] Korhonen 2009, s. 18.
[27] Saarenpää 2000, s. 48; Saarenpää 2003, s. 308—311 ja Pöysti 1999, s. 399.
[28] HE 309/1993 vp, s. 42.
[29] Neuvonen 2014, s. 16; Korhonen 2003, s. 108—113 ja Saarenpää 1997, s. 270.
[30] Wasserstrom 1978, s. 148 ja Blume 1997, s. 197.
[31] McGeveran 2016, s. 3 ja Neuvonen 2014, s. 16—17.
[32] Neuvonen et al. 2015, s. 28—29. Riku Neuvonen ja Pauli Rautiainen erottelevat eksplisiittiset ja implisiittiset perusoikeudet siten, että implisiittiset perusoikeudet eivät löydy eksplisiittisesti kirjoitettuna perustuslain perusoikeusluettelosta eksplisiittisten perusoikeuksien tapaan, mutta ne ovat silti konstruoitavissa perusoikeuksiksi. Näkemykseni mukaan yksityisyyden suoja oli alun perin implisiittinen perusoikeus, joka myöhemmin kirjattiin perus- ja ihmisoikeusinstrumentteihin eksplisiittiseksi perusoikeudeksi.

ensimmäiset laajemmat ilmentymät nähtiin kuitenkin yhdysvaltalaisessa prosessioikeudessa erityisesti rikosprosesseihin liittyvinä vaatimuksina olla käyttämättä tiettyä todistusaineistoa Yhdysvaltain perustuslain neljännen lisäyksen nojalla.[33] Mainituissa tapauksissa kyse on ollut ennen kaikkea tarpeettomaksi katsotun tiedon etsimisestä ja takavarikoimisesta.

Sitä voidaan pitää kuitenkin hyvin ymmärrettävänä, että Suomessa kiinnostus yksityisyyteen oikeudellisessa mielessä heräsi nimenomaan henkilö- ja hallinto-oikeudellisessa tutkimuksessa, sillä myös Yhdysvalloissa kyse oli pohjimmiltaan yksityisyyden konstruoimisesta salassa pidettävän tiedon ja päätöksenteon pohjalta perusoikeudelliseksi käsitteeksi.[34] Kyse oli alun perin nimenomaan julkisen vallan rajoittamisesta yksilön suojelemiseksi vallan väärinkäyttöä vastaan.[35] Sittemmin yhdysvaltalaisessa oikeuskäytännössä ja -tutkimuksessa alettiin nähdä yhä selvemmin yhteys myös omistusoikeuden ja yksityisyyden välillä.[36] Näin yksityisyys alkoi eriytymään yksityiselämän suojasta, taustalla ajatus kotirauhan piirissä olevien asiapapereiden ja tavaroiden suojelemisesta. Toisena yksityisyyteen kuuluvana elementtinä alkoi muodostua ajatus kodin ulkopuolelle suuntautuvan viestinnän luottamuksellisuuden takaamisesta.[37]

Edellä mainittuihin oikeustapauksiin viitaten yksityisyys oikeudellisena käsitteenä alkoikin kehittyä ennen muuta yksilön suojaamisesta kotirauhan piirissä tapahtuvaa viranomaisen suorittamaa salakuuntelua vastaan. Sittemmin kysymyksiä on herättänyt vuonna 1792 voimaan tulleen Yhdysvaltain perustuslain (*U.S. Constitution)* tarpeetonta kotietsintää ja takavarikkoa koskevan neljännen lisäyksen tulkinta teknologian kehittyessä, erityisesti ottaen huomioon uuden teknologian mahdollistamat kotirauhan piiriin kodin ulkopuolelta suunnatut kuuntelumenetelmät. Toisaalta uudet teknologiset edistysaskeleet, kuten telekommunikaatio ja myöhemmin internet, lisäsivät painetta yksityisyyden käsitteen laajemmalle tulkinnalle siten, ettei kyse olisi ainoastaan kotirauhan piirissä suojatusta yksityisyydestä. Näin ollen Yhdysvaltain kongressi sääti ensimmäisen viestintälain[38] vuonna

---

[33] Ks. Olmstead v. United States 277 U.S. 438 (1928) Yhdysvaltain perustuslain neljännen lisäyksen tulkinnasta ja IV Amendment: "*The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."*

[34] McGeveran 2016, s. 3—7.

[35] Weems v. United States, 217 U.S. 349, 373, 30 S. Ct. 544, 551 (54 L. Ed. 793, 19 Ann. Cas. 705) ja McCulloch v. Maryland, 4 Wheat. 316, 407 4 L. Ed. 579.

[36] McGeveran 2016, s. 9.

[37] McGeveran 2016, s. 9; ks. myös Goldman v. United States, 316 U.S. 129 (1942) havainnollistava esimerkkinä kotirauhan piirissä olevan yksityisyyden suhteesta kotirauhan ulkopuolella suojattavan yksityisyyden tasoon. Kun kyseisessä tapauksessa yksityisyyttä ei katsottu tulleen loukatuksi, koska yksilön henkilökohtaisia tietoja ei kerätty tunkeutumalla tämän kotirauhan piiriin, tapauksessa Silverman v. United States, 365 U.S. 505 (1961) yksityisyyden suojan nähtiin tulleen loukatuksi, kun kuuntelulaite oli asennettu väliseinän sisälle, jolloin kyseessä olikin lainvastainen tunkeutuminen toisen kotirauhan piiriin ja salakuuntelussa oli ollut näin ollen kyse yksityisyyden loukkauksesta: *"a violation of the Fourth Amendment based on Olmstead v. United States"*.

[38] Communication Act of 1934.

1934, joka käsitteli sekä tele- että radioyhteyksiä ja niissä tapahtuvan kommunikaation luottamuksellisuutta ja yksityisyyttä.

Yksityisyys nähtiin yhä enenevässä määrin rikosprosesseihin liittyvänä käsitteenä, kun siihen pohjautuen alettiin rakentaa uutta tulkintalinjaa Yhdysvaltain perustuslain viidennen lisäyksen osalta. Kyse oli ennen kaikkea oikeudenmukaisen oikeudenkäynnin toteuttamisesta rajoittamalla hallinnollisia tiedonhankintakeinoja, jotta rikoksesta epäillyn yksityisyyteen ei voitaisi puuttua tarpeettomalla tai muuten epäoikeudenmukaisella tavalla.[39] Näin alkoi vähitellen kehittyä ajatus siitä, että yksilön yksityisyyteen puuttuminen edellyttää lainsäädännöllistä tukea.

Yksityisyyden suojan muodostuessa perusoikeudeksi, voidaan edellä mainittuun viitaten käänteisesti todeta, että yksilön perus- ja ihmisoikeustasoiseen yksityisyyden suojaan kajoaminen edellyttää tarkkarajaista ja täsmällistä lainsäädäntöä. Yhdysvaltain korkein oikeus alkoi lopulta vuodesta 1973 lähtien tulkitsemaan oikeutta yksityisyyteen erillisenä perusoikeutena.[40] Vuonna 1983 tapauksessa United States v. Karmer[41] yksityisyyden elementeiksi määrittyivät yksilön oikeus rauhaan, vapaus olla joutumatta julkisen valvonnan kohteeksi sekä yksilön oikeus pidättäytyä julkisuudesta. Kyse on tällöin ennen kaikkea henkilökohtaiseen turvallisuuteen, vapauteen ja omaisuuden suojaan läheisesti liittyvästä perusoikeudesta.[42]

Näitä yksityisyyden kansainvälisiä perinteitä kunnioittaen Suomessa vuoden 1995 hallitusmuodon (HM, 94/1919) perusoikeusuudistuksen yhteydessä uutena perusoikeutena suojattiin jokaisen yksityiselämä.[43] Suomessa yksityiselämän suojaan kuuluvina elementteinä on nähty kunnian suoja, viestinnän luottamuksellisuus sekä kotirauha. Kyse on sekä fyysisestä vapaudesta että itsemääräämisoikeudesta ja tahdon vapaudesta.[44]

Tietoon liittyvänä ihmisoikeutena oikeus yksityisyyteen on joutunut monesti informaatioon liittyvien vapausoikeuksien kategoriaan kuuluvien ihmisoikeuksien kanssa konfliktiin.[45] Oikeutta yksityisyyteen on jouduttu punnitsemaan erityisesti yksilön sananvapautta vasten. Kuten edellä on kuvattu, oikeus yksityisyyteen on kehittynyt erityisesti yksilön oikeutena yksityiselämän suojaan vertikaalisessa suhteessa julkiseen valtaan nähden. Yksityisyys nousee kuitenkin nykypäivänä esille

[39] McGeveran 2016, s. 9—11 ja ks. myös United States v. Hubbell, 530 U.S. 27, 30-38 (2000) ja United States v. John Doe, 670 F.3d 1335, 1337 (11th Cir. 2012), Grand Jury Subpoena Duces Tecum Dated March 25, 2011 (2012) sekä V Amendment.
[40] Roe v. Wade 410 U.S. 113 (1973): Tapauksessa tutkittiin aborttioikeutta osana yksityisyyttä, mistä ilmenee yksityisyyden läheinen yhteys henkilökohtaiseen vapauteen ja itsemääräämisoikeuteen.
[41] United States v. Karmer, 711 F.2d 789, 792 (7th Cir.), cert. denied, 464 U.S. 962 (1983).
[42] Nestlerode 1993, s. 63.
[43] HE 309/1993 vp, s. 17 ja Sarja 2008, s. 793.
[44] HE 309/1993 vp, s. 17.
[45] AOA dnro 2447/4/05: Kyse oli terveyskeskuksen ylilääkärin menettelystä valokuvaamisen kieltämisessä, jossa yksityisyys julkisissa tiloissa punnittuna sananvapautta vasten johti siihen, että tällaisissa tiloissa kuvaaminen ei voi olla ennakkoluvanvaraista.

yhä useammin toisten yksilöiden välillä horisontaalisessa suhteessa. Lisäksi on huomattava, että yksityisyyteen nähdään nykyisin kuuluvan myös oikeus tietää ja määrätä itseään koskevien tietojen käytöstä sekä tietosuojasta. Kyse on oikeudesta järjestää yksityiselämänsä siten, ettei ulkopuolinen voi perusteettomasti puuttua siihen, ja oleskella määrätyllä alueella ilman ulkopuolisten häirintää, katselua, kuuntelua tai muuta puuttumista. Tarkoituksena ei ole siis säännellä tietyn tyyppisiä tietoja salassa pidettäviksi, sillä yksityisyys on yksilön oikeus, joka ei ole riippuvainen suojattavien tietojen sisällöstä, vaan yksilön henkilökohtaisesta oikeudesta yksityisyyteen erilaisten oikeuksien, kuten oikeudesta henkilötietojen suojaan, yhdistelmänä.[46]

### 1.2. Oikeus henkilötietojen suojaan

Vanhastaan oikeuskirjallisuudessa on katsottu yksityisyyteen sisältyvän useita eri elementtejä. Yleisintä on liittää yksityisyys yksilön autonomiaan, itsemääräämisoikeuteen ja ainutlaatuiseen henkilöyteen. Vaikka henkilötietojen suojalle on olemassa monenlaisia eri tulkintalinjoja, on useimmiten lähdetty siitä, että kyse on yksilöllisyyteen pohjautuvasta alun perin implisiittisestä oikeudesta. Yksityisyyshän viittaa siihen, mikä on yksilölle henkilökohtaista. Oikeus yksityisyyteen ihmisoikeutena on yksi keskeisimpiä ihmisoikeuksia muun muassa siksi, että siihen sisältyy jokaisen vapaus elää haluamallaan tavalla ja muokata identiteettiään sekä olemustaan oma-aloitteisesti. Henkilötietojen suojan ja yksityisyyden osalta uhkakuvana on nähty erityisesti vertikaalinen huolenaihe siitä, että valtio valvoo yksilöiden tekemisiä ja horisontaalisesti muut yksilöt hyödyntävät toisten henkilökohtaisia tietoja.[47]

Oikeus yksityisyyteen nähdään soveltamisalaltaan laajempana käsitteenä kuin henkilötietojen suoja. Henkilötietojen suojaamisessa on kysymys tunnistettavien henkilöiden eli rekisteröityjen tietojen suojaamisesta.[48] Yksityisyydestä eroten, oikeutta henkilötietojen suojaan ei ole olemassa ennen kuin yksilöä koskevia tietoja on kerätty tai dokumentoitu. Henkilötietojen kerääminen ja dokumentoiminen on jo itsessään henkilötietojen käsittelyä, joten sen on tapahduttava tietosuojalainsäädännön sallimissa rajoissa. Tarkoituksena on suojata yksilöä epäoikeudenmukaiselta tietojen kerääämiseltä, käytöltä ja säilyttämiseltä.[49]

On myös syytä huomata, että vaikka henkilötietojen suoja sekä yksityisyys molemmat suojaavat yksilöä horisontaalisessa ja vertikaalisessa suhteessa, henkilötietojen suoja keskittyy nimenomaisesti henkilötietoja käsittelevien toimintaan. Varsinkin teknologisen kehityksen myötä muodostuneessa verkkoyhteiskunnassa on ollut tarpeen muodostaa oma yksityisyydestä erillään oleva perus-

[46] Aarnio 2002, s. 6—12; Aarnio 2007, s. 15—18; HE 49/1986 vp, s. 3; HE 239/1997 vp, s. 5.
[47] Lindroos-Hovinheimo 2018, s. 58.
[48] Mayer-Schönberger et al. 2013, s. 11—15.
[49] Ferretti 2014, s. 848—849; ks. myös Kokott et al. 2013, s. 222—228 yksityisyyden ja henkilötietojen suojan välisestä erosta.

oikeus, henkilötietojen suoja. Lähtökohtana oli henkilötietoja käsitteleville tahoille suunnattu sääntely tietojen käsittelyn läpinäkyvyyden varmistamiseksi. Lisäksi tarkoituksena on ollut mahdollistaa yksilöille monenlaisia spesifimpiä oikeuksia, kuten oikeus hallita omia henkilötietojaan ja niiden hyödyntämistä. Tausta-ajatus on silti sama eli yksilön koskemattomuuden ja vapauden suojeleminen.[50]

Oikeudesta henkilötietojen suojaan on muotoutunut yksi keskeisimmistä informaatioon liittyvistä tiedollista itsemääräämisoikeutta vahvistavista perusoikeuksistamme viime vuosina.[51] Globaalisti on kehittynyt painetta säännellä tietojenkäsittelyä yhä kattavammin erityisesti teknologisen kehityksen ja sen mahdollistamien uusien tietojenkäsittelykeinojen myötä.[52] Uusi sääntely on ollut välttämätöntä teknologisen kehityksen seurauksena syntyneen tietojen keräämisen ja hyödyntämisen tehostumisen johdosta. Henkilötietojen käsittelystä on tullut niin keskeinen sääntelyn kohde, ettei enää voida puhua pelkästään oikeudesta yksityisyyteen, vaan sen lisäksi on muotoutunut erityinen perusoikeus eli oikeus henkilötietojen suojaan vastauksena nykyisen verkkoyhteiskunnan muodostamiin haasteisiin.

Kuten todettu, yksityisyyden käsite oikeudellisena instituutiona on lähtöisin Yhdysvalloista. Samoin yksityisyydestä johdetun perusoikeuden henkilötietojen suojaan on nähty juontavan juurensa Yhdysvalloista. Kuitenkin oikeudellisena käsitteenä tietosuoja nimenomaan ihmisoikeustasoisesti on enemmän eurooppalaisen oikeuskehityksen tulosta. Alkusysäyksen henkilötietojen käsittelyn sääntelylle loivat yksilöiden yksityisyyteen vaikuttavien toimenpiteiden ja toiminnallisuuksien kehittyminen, erityisesti väestönlaskentaan ja hallinnollisiin asiakirjoihin kohdistuviin käsittelytoimiin liittyen.[53] Toinen keskeinen lainsäädännöllistä painetta luonut kokonaisuus on ollut postijärjestelmän sekä telekommunikaation kehitys.[54]

Lopulta vuonna 1960 Yhdysvalloissa kehittyi näkemys siitä, että on olemassa neljänlaisia henkilötietojen käsittelyyn liittyviä vahingonkorvaustapauksia, keskeisimpinä näistä yksityiselämään kuuluvien tosiseikkojen julkistaminen sekä virheellisten henkilötietojen levittäminen.[55] Käsillä on yksi

[50] Lindroos-Hovinheimo 2018, s. 59.
[51] Neuvonen 2014, s. 66—68.
[52] Ks. esim. Solove 2006, s. 3: *"Today, we have hundreds of laws pertaining to privacy: the common law torts, evidentiary privilege, constitutional law, at least twenty federal statutes, and numerous statutes in each of the fifty states."*
[53] Ibid. s. 7.
[54] Kirjepostin luottamuksellisuutta alettiin säännellä Yhdysvalloissa jo vuonna 1825 (42 U.S. Code § 1702). Kyseinen laki on vieläkin voimassa. Laissa todetaan muun muassa, että "*whoever takes any letter, postal card, or package out of any post office or any authorized depository for mail matter, or from any letter or mail carrier, - - before it has been delivered to the person to whom it was directed, with design to obstruct the correspondence, or to pry into the business or secrets of another, or opens embezzles, or destroys the same, shall be fined - - or imprisoned".*
[55] Ks. Prosser 1960, s. 383—391, jossa William Prosser listaa seuraavat neljä vahingonkorvaustyyppiä: 1. Intrusion upon seclusion, 2. public disclosure of private fact, 3. false light or "*publicity*" 4. appropriation.

varhaisimmista henkilötietojen suojaa koskevista ilmentymistä, sillä tapauksissa oli kyse jostain sellaisesta yksilön yksityisyyden suojelemisesta, jota ei voida konstruoida ennen kuin yksilöä koskevia tietoja on kerätty tai dokumentoitu jollekin alustalle. Kysymyksessä ei siis ollut yksityisyyden suojeleminen klassisessa mielessä, kun yksityisyys ei edellytä mitään tiettyä alustaa, jolle tallennettuja tietoja olisi suojattava. Tällöin tietylle alustalle rekisteröityjen tietojen nähtiin olevan sellaisen oikeudellisen suojelun kohteena, minkä ei välttämättä nähty muodostuvan puhtaasti henkilön yksityiselämän suojasta[56].

Henkilötietojen suojan vakiintumisen eurooppalaiseksi perusoikeudeksi voidaan nähdä saaneen alkunsa 1970-luvun alussa automatisoidun tietojenkäsittelyn synnyttämästä huolesta. Tämä johti lainsäädäntöpaineeseen useissa Euroopan valtioissa, eikä tietotekninen kehityskään toisaalta hidastunut 1970-luvun edetessä. Uhkakuvien vertikaalinen luonne on korostunut, kun 1990- ja 2000-luvulla teknologinen kehitys on mahdollistanut yhä laajemman julkisen vallan suorittaman valvonnan esimerkiksi terrorismin ja rikollisuuden torjunnan nimissä. Sittemmin henkilötietojen suojan asema perusoikeutena on korostunut erityisesti Euroopan unionin ja sen jäsenvaltioiden kansallisessa sääntelyssä.

Henkilötietojen suojaa koskevan sääntelyn voidaan katsoa olevan pitkälti hallinto- sekä informaatio-oikeudellista. Nykyisin on mahdollista puhua myös oikeusinformatiikasta, mutta suurin osa henkilötietojen suojaa koskevasta tarkemmasta teknisestä sääntelystä kuuluu nimenomaisesti hallinto-oikeuden alaan.[57] Monissa oikeustieteellisissä tutkimuksissa vielä nykyäänkin tietosuojan on nähty kuuluvan Euroopassa hallinto-oikeuden alueelle.[58]

Eurooppalaista henkilötietojen suojan historiallista taustaa tutkittaessa esille nostetaan yleensä yksilöiden suojelua henkilötietojen automaattisessa tietojen käsittelyssä koskeva yleissopimus (*Euroopan neuvoston tietosuojasopimus*), OECD[59]:n vuonna 1980 hyväksymä yksityisyyden suojelemista ja kansainvälistä henkilötietojen siirtämistä koskeva suositus (*OECD:n tietosuojasuositus*) ja Euroopan unionin tietosuojalainsäädäntö, erityisesti henkilötietodirektiivi. Sääntelytarkkuutta tarkasteltaessa voidaan todeta eurooppalaisen tietosuojalainsäädännön olleen hyvin periaatelähtöistä eli sääntelykeinoltaan oikeudellisten periaatteiden sävyttämää. Varhaisimpia tietosuojaoikeudellisia periaatteita ovat olleet laillisuus-, lainalaisuus-, suhteellisuus- sekä käyttötarkoitussidonnaisuusperiaate. Tietosuojaperiaatteiden voidaan todeta ottaneen merkittävästi vaikutteita hallinto-oikeu-

[56] Huomaa erityisesti tutkielman II osan yksityisyyttä käsittelevässä kappaleessa 1.1. mainittu kehityssuunta, jossa yksityisyyteen liitettiin omaan informaation kohdentuva omistusoikeus.
[57] Koillinen 2013, s. 172.
[58] Hildebrandt 2008, s. 324. Vrt. Voutilainen 2012, s. 144—145.
[59] Taloudellisen yhteistyön ja kehityksen järjestö (engl. *Organisation for Economic Co-operation and Development*).

den yleisistä opeista, mikä johtunee siitä, että alkujaan eurooppalaista tietosuojalainsäädäntöä kehitettäessä nähtiin tarpeellisena suojata yksilöitä nimenomaan vertikaalisessa suhteessa eli julkista valtaa vastaan.[60]

Suomalaisessa oikeushistoriassa tietosuoja on nähty kiintoisana tutkimuksen kohteena esimerkiksi verotukseen, sosiaali- ja terveydenhuoltoon sekä perusrekistereihin liittyen. Yksityistä sektoria koskevissa varhaisimmissa tietosuojaa käsittelevissä oikeudellisissa tutkimuksissa kiinnostuksen kohteena ovat olleet erityisesti rahoituslaitokset, työelämä ja markkinointi.[61] Suomessa kuten muuallakin Euroopassa henkilötietojen suoja alkoi kehittyä eräänlaisena yksityisyyden ja yksityiselämän suojan sovellutuksena. Lisäksi vielä kehityksen alkuvaiheessa pohdittiin sitä, onko tietosuoja perusoikeutena nimenomaisesti luonnollisten henkilöiden tietojen suojelemista koskeva oikeus, kun etsittiin eroavaisuuksia yksityisyyden ja tietosuojan välille.

Monesti erottelua yksityisyyden ja tietosuojan välillä on pidetty yksin teoreettisena ja akateemisena kysymyksenä, sekä lisäksi käytännön oikeusdogmatiikan kannalta tietosuoja ja yksityisyys nähtiin jopa toistensa synonyymeinä. On kuitenkin huomattava, että siinä missä yksityisyys suojaa yksilön yksityisyyselämää perusteettomalta puuttumiselta, suojaa henkilötietojen suoja yksilöä perusteettomalta henkilötietojen keräämiseltä, käyttämiseltä ja luovuttamiselta sekä antaa oikeuden hallita laajemmin omien henkilötietojen käsittelyä.

Ennen Euroopan unionin yleisen tietosuoja-asetuksen säätämistä henkilötietojen suoja on monella tapaa asteittain kehittynyt kohti nykytasoa. Nimenomaan eurooppaoikeudessa oikeus henkilötietojen suojaan on nähty omana erillisenä perusoikeutena, joka ansaitsee maininnan unionin perusoikeuskirjassa (2012/C 326/02). Toisaalta kyse on myös siitä, että aikaisemmin implisiittisenä, eksplisiittisesti kirjoitetuista perusoikeuksista johdetavissa olevana, nähty oikeus henkilötietojen suojaan tuli perusoikeuskirjan myötä eksplisiittiseksi perusoikeudeksi unionin alueella.[62] Kansainvälisesti ei ole kuitenkaan vielä itsestään selvää, voidaanko henkilötietojen suojaa pitää yksityisyydestä erillään olevana itsenäisenä perusoikeutena. Esimerkiksi Euroopan ihmisoikeussopimuksessa[63]

---

[60] Brygrave 2002, s. 119; Koillinen 2013, s. 173 ja Brouwer 2010, s. 280.

[61] Koillinen 2013, s. 174; huomaa myös Sorvari 2002, esimerkkinä henkilötietojen suojaa käsittelevästä tutkimuksesta markkinoinnin perspektiivistä.

[62] Ks. esim. Neuvonen et al. 2015, s. 29 ja 33—34, implisiittisistä ja eksplisiittisistä perusoikeuksista. Artikkelissa Riku Neuvonen ja Pauli Rautiainen toteavat oikeusteoreettisessa tutkimuksessaan, että henkilötietojen suojassa on ollut kyse implisiittisestä perusoikeudesta. Artikkelissa tietosuojan todetaan olevan vielä edelleen Suomen perustuslakia tarkasteltaessa implisiittinen perusoikeus. Näkemykseni mukaan eurooppaoikeudellisessa kontekstissa kyse on kuitenkin nykyisin eksplisiittisestä perusoikeudesta, sillä oikeus henkilötietojen suojaan mainitaan nykyisin erikseen perusoikeuskirjan 8 artiklassa yksityisyyden suojasta erillisenä perusoikeutena. Käytännössä unionin Perusoikeuskirja on kuitenkin maailmanlaajuisesti ainoita perusoikeusinstrumentteja, jossa oikeus henkilötietojen suojaan mainitaan itsenäisenä perusoikeutena, joten globaalilla tasolla voidaan katsoa tietosuojan olevan edelleen suurimmassa osassa valtioyhteisöä implisiittinen perusoikeus, joka kuitenkin saatetaan mainita yksityiselämän suojan elementtinä.

[63] EIS annettiin 4.11.1950 ja Suomi liittyi sopimukseen toukokuussa 1989. Sopimus tuli Suomessa sitovana voimaan vuotta myöhemmin siihen liittymisestä.

(EIS, SopS 63/1999) henkilötietojen suojaa ei ole määritelty erilliseksi ihmisoikeudeksi. Suomi liittyi Euroopan ihmisoikeussopimukseen vuonna 1989, mutta sopimusta on sittemmin muutettu lisäpöytäkirjoilla, joilla ei ole kuitenkaan merkittävää vaikutusta yksityisyyden ja tietosuojan kannalta.

Perusoikeuskirjan[64] 8 artiklan mukaan henkilötietojen käsittelyn tulee olla ”*asianmukaista ja sen on tapahduttava tiettyä tarkoitusta varten ja asianomaisen henkilön suostumuksella tai muun laissa säädetyn oikeuttavan perusteen nojalla. Jokaisella on oikeus tutustua niihin tietoihin, joita hänestä on kerätty, ja saada ne oikaistuksi*.” Perusoikeuskirjan 8 artiklan sanamuodosta on huomattavissa, että kyseessä on nimenomaisesti henkilötietoja käsitteleville tahoille asetettu toimeksianto käsitellä henkilötietoja asianmukaisesti ja antaa rekisteröidyille mahdollisuuden käyttää tiettyjä oikeuksiaan, kun näiden henkilötietoja käsitellään. Yksityisyys puolestaan suuntautuu laajemmalle, ja se ei tule huomioiduksi pelkästään rekisterinpitäjän tai henkilötietojen käsittelijän toiminnassa. Toisaalta yksityisyyden suoja ei anna yksilölle erityisiä oikeuksia hallita omien tietojensa hyödyntämistä.[65]

Unionin tasolla henkilötietojen suojasta on katsottu muodostuneen perusoikeus viimeistään sen tullessa osaksi unionin perusoikeuskirjaa.[66] Tätä aikaisemminkin Euroopan unionissa oli pantu täytäntöön laajaa henkilötietojen käsittelyä koskevaa harmonisointia. Eurooppalaisessa katsannossa henkilötietojen käsittelyn sääntely sai alkusysäyksensä vuonna 1995 säädetyn henkilötietodirektiivin myötä. Direktiivin tarkoituksena oli suojella henkilötietojen käsittelyn kohteena olevia yksilöitä sekä säännellä näiden tietojen vapaata liikkuvuutta.[67] Henkilötietodirektiivin johdanto-osan 2 kappaleessa todetaankin, että ”*tietojenkäsittelyjärjestelmät on tehty palvelemaan ihmistä; järjestelmiä käytettäessä on kunnioitettava yksilöiden perusoikeuksia ja -vapauksia heidän kansalaisuudestaan tai asuinpaikastaan riippumatta, erityisesti oikeutta yksityisyyteen, ja osallistuttava taloudelliseen ja sosiaaliseen kehitykseen, kaupan kehittämiseen sekä yksilöiden hyvinvoinnin lisäämiseen”.* Näin ollen voidaan todeta, että henkilötietojen suojan tasoa on arvioitava nimenomaan rekisteröitynä olevan yksilön näkökulmasta. Henkilötietojen suoja on itsenäinen perusoikeus, jota tulee punnita muiden perusoikeuksien tapaan konfliktitilanteissa tilanteissa suhteessa muihin perus- ja ihmisoikeuksiin.

Ennen henkilötietodirektiivin säätämistä Euroopan unionin tuomioistuinkäytännössä ei oltu vielä erotettu tietosuojaa yksityisyydestä. Henkilötietojen suojan muodostuminen perusoikeudeksi alkoi-

[64] Euroopan unionin perusoikeuskirjasta tuli velvoittava Lissabonin sopimuksen myötä vuonna 2009.
[65] Lindroos-Hovinneva 2018, s. 59.
[66] Ks. esim. González Fuster 2014, s. 253—261.
[67] Näin todetaan muun muassa Euroopan tietosuojavaltuutetun verkkosivuilla (EDPS, *European Data Protection Supervisor*): https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en.

kin vasta henkilötietodirektiivin säätämisen jälkeen. Sitä aikaisemmin Euroopassa oli kuitenkin tiettyjä viitteitä tietosuojan perusoikeustasoisesta olemassa olosta.[68] Vaikka Euroopan ihmisoikeussopimuksessa ei ollutkaan henkilötietojen suojaa koskevaa mainintaa, on Euroopan ihmisoikeustuomioistuin katsonut ratkaisussaan Leander v. Ruotsi vuonna 1987, että henkilötietojen suoja nauttii ihmisoikeustasoista suojaa sen kuuluessa yksityisyyden suojaa turvaavan Euroopan ihmisoikeussopimuksen 8 artiklan alaan. Selvennys oli tarpeellinen, sillä 1980-luvun alussa Euroopan neuvosto päätti säätää henkilötietojen suojasta ihmisoikeusinstrumentin sijaan erillisessä tietosuojasopimuksessa.[69]

Suomessa henkilötietolain säätämisen yhteydessä omaksuttiin malli, jonka mukaan muut yksityisyyteen liittyvät suojattavat oikeudet sisällytettiin yksityiselämän suojan alle, kuten henkilötietolain 1 §:ssä sen soveltamisalasta todetaan: ”*tarkoituksena on toteuttaa yksityiselämän suojaa ja muita yksityisyyden suojaa turvaavia perusoikeuksia.*” Tämä voidaan nähdä selkeänä erona verrattuna henkilötietolakia edeltäneeseen henkilörekisterilakiin, jonka soveltamisalaa koskevassa säännöksessä ei vielä todettu laissa olevan kyse minkään perusoikeuden suojaamisesta. On huomattava, että Suomen oikeusjärjestelmässä henkilötietojen suoja perusoikeutena muodostui vasta vuoden 1995 perusoikeusuudistuksessa.[70]

Vahvistusta yksityisyyden ja henkilötietojen suojan välisen kytkennän katkaisemisemiseksi on tuonut kansainvälisellä tasolla muun muassa Yhdistyneen kuningaskunnan oikeuskäytäntö. Sen mukaan on katsottu yksityisyyden ja henkilötietojen suojan välisen yhteyden ylläpitämisen rajoittavan suojattavien tietojen joukkoa, jota ei puolestaan voida pitää perus- ja ihmisoikeusmyönteisen lain-tulkinnan mukaisena.[71] On huomattava, että tietosuojan on tarkoitus suojata kaikkia sellaisia tietoja, jotka ovat yhdistettävissä tiettyyn henkilöön, kun taas yksityisyydellä suojataan luonnollisen henkilön yksityiselämään vaikuttavia toimia. Toisin sanoen tietosuojaan ei kytkeydy minkäänlaista vaikuttavuusvaatimusta, vaan riittävää on, että henkilö on yhdistettävissä tiettyyn tietoon.[72] Samankaltaiseen johtopäätökseen tultiin Euroopan unionin tuomioistuimen ratkaisussa komissio v. Bavarian Lager, jossa unionin tuomioistuin totesi, että kaikki henkilötiedot eivät välttämättä kuulu yksityiselämän käsitteen alaan.[73] Unionin oikeus näyttääkin pakottavan myös Suomen omaksumaan käsityksen tietosuojasta erillisenä perusoikeutena, jollaisena se ilmaistaan kaikissa jäsenvaltioissa suoraan sovellettavan yleisen tietosuoja-asetuksen johdanto-osan 2 kappaleessa.

[68] González Fuster 2014, s. 111—162.
[69] Gurtwith et al. 2009, s. 24 ja Koillinen 2013, s. 177.
[70] HM:n 8 § ja nykyisin PL:n 10.1 §.
[71] Brownsword et al. 2009, s. 75.
[72] Tzanou 2010, s. 38.
[73] EUT: Komissio v. Bavarian Lager C-28/08, kohta 118.

### 1.3. Julkisuusperiaate

Julkisuusperiaate voidaan nähdä eräänlaisena vastinparina yksityisyydelle ja henkilötietojen suojalle varsinkin edellä mainittuja tarkasteltaessa salassapidon näkökulmasta. Siinä missä yksityisyys ja henkilötietojen suoja vaikuttavat vahvasti myös yksilöiden välillä horisontaalisessa suhteessa, julkisuusperiaate[74] vaikuttaa ennen kaikkea vertikaalisessa suhteessa ja sen kautta on tarkoituksena säännellä yksilön oikeutta tietoon perus- ja ihmisoikeustasoisesti. Julkisuusperiaatteella on kuitenkin nähty olevan eräitä kiinnekohtia myös horisontaaliseen sääntelyyn erityisesti liittyen yksityisoikeuden alaan kuuluvaan tekijänoikeussääntelyyn. Nykyisin julkisuusperiaatetta säännellään yleislakina toimivassa viranomaistoiminnan julkisuudesta annetussa laissa (*julkisuuslaki*, 621/1999). Periaatteella on kuitenkin pitkä historia.

Moderni julkisuusperiaate on demokraattisen yhteiskunnan perustavanlaatuinen toiminta- ja rakenneperiaate, johon kuuluu useita laadullisia elementtejä kuten tiedon saannin oikeus ja mahdollisuus. Kyse on julkisen tiedon saamisesta, viestinnästä ja ilmaisun vapaudesta sekä mielipiteen muodostamisesta kuten myös julkiseen keskusteluun osallistumisesta ja sen edellytyksistä erinäisin välinein. Julkisuusperiaatteeseen sisältyy jokaisen oikeus päästä viranomaisen säilyttämiin julkisiin tietovarantoihin, velvollisuus luovuttaa pyydetyt julkiset tiedot sekä proaktiivinen julkisuus, jolla tarkoitetaan viranomaisen velvollisuutta aktiivisesti ja oma-aloitteisesti tiedottaa toiminnastaan. Hallinto-oikeudellisessa tutkimuksessa julkisuusperiaatteen toteuttamistapoja on nykyisin nähty olevan asiakirjajulkisuus, viranomaisen tiedottaminen ja asianmukaisen tietohallinnon järjestäminen. Keskeisimpänä julkisuusperiaatteen toteutumismuotona asiakirjajulkisuus jakaantuu edelleen asianosaisjulkisuuteen ja yleisöjulkisuus. Yleisöjulkisuus viittaa käsittelyn julkisuuteen.[75]

Pohjoismaisessa katsannossa julkisuusperiaatetta on sananvapauden ohella pidetty yhtenä keskeisimmistä perusoikeuksista ja oikeusperiaatteista demokraattiselle yhteiskunnalle. Tässä suhteessa julkisuusperiaatetta voidaan pitää eräänlaisena demokraattisen valtion tunnuspiirteenä. Toisaalta demokratian näkökulmasta julkisuusperiaate tarvitsee tuekseen sananvapauden, jonka nojalla yksilöt voivat ilmaista julkisuusperiaatetta käyttäen muodostetun mielipiteensä. Kyse on ennen kaikkea yksilön oikeudesta saada luotettavaa tietoa julkista valtaa käyttävien viranomaisten ja muiden julkisten organisaatioiden toiminnasta, näiden toimien vaikutuksista sekä laajemmin yhteiskuntaoloista.[76] Tällainen aineisto voi sisältää myös henkilötietoja.

---

[74] Julkisuuslain 1.1 §:n mukaan julkisuusperiaatteella tarkoitetaan sitä, että *"viranomaisten asiakirjat ovat julkisia, jollei tässä tai muussa laissa erikseen toisin säädetä".* Lain soveltamisalaa koskevan 2.1 §:n mukaan julkisuuslaissa *"säädetään oikeudesta saada tieto viranomaisten julkisista asiakirjoista sekä viranomaisessa toimivan vaitiolovelvollisuudesta, asiakirjojen salassapidosta ja muista tietojen saantia koskevista yleisten ja yksityisten etujen suojaamiseksi välttämättömistä rajoituksista samoin kuin viranomaisten velvollisuuksista tämän lain tarkoituksen toteuttamiseksi."*

[75] Mäenpää 2016, s. 3—4 ja 18—19.

[76] HE 30/1998 vp, s. 9 ja Korhonen 2003, s. 36.

Myös henkilötietojen suojaan katsotaan kuuluvan oikeuden saada nähtävilleen itseään koskevia tietoja sekä vastaanottaa informaatiota omien henkilötietojensa käsittelystä. Julkisuusperiaate on kuitenkin siinä mielessä laajempi, että siihen sisältyy jokaisen oikeus saada tietoa sellaisestakin viranomaisen toiminnasta, joka ei välttämättä koske tiedon pyytänyttä henkilöä. Erityisesti asiakirjajulkisuutta voidaan pitää tietosuojaan sisältyvää läpinäkyvyyttä laajempana, sen tarkoittaessa jokaisen oikeutta saada tietoa viranomaisen asiakirjasta, joka on julkinen. Käsittelyjulkisuus puolestaan tarkoittaa yksilön oikeutta seurata asioiden käsittelyä julkista valtaa käyttävissä organisaatioissa, kun taas asianosaisjulkisuus tarkoittaa asianosaisen oikeutta tutustua aineistoon, joka on kertynyt häntä itseään koskevassa asiassa.[77]

Julkisuusperiaatteen juuret löytyvät paljon kauempaa historiasta verrattuna edellä käsiteltyyn yksityisyyteen ja henkilötietojen suojaan. Erityisesti 1500-luvulla laajempaan käyttöön tulleen kirjapainotaidon myötä syntyi painetta tarkastella, minkälainen tieto on ylipäänsä julkista ja mitä asioita yksilöllä on oikeus saada tietoonsa. Myös Ruotsi-Suomessa vallitsi monarkioille tyypillinen salaamiskulttuuri. Voidaankin ajatella, että tuohon aikaan kyse oli julkisuusperiaatteen sijaan pikemminkin salaamisperiaatteesta. 1600- ja 1700-lukujen edetessä Ruotsi-Suomelle olikin tyypillistä erilaiset sensuuri- ja ennakkovalvontajärjestelmät.[78] Liberaalimman ajattelun myötä syntyi kuitenkin tarve säätää lakeja, joilla pyrittiin lisäämään yksilöiden oikeusturvaa sekä oikeusvarmuutta vaikeasti ennakoitavan sensuurin rationalisoimiseksi.[79]

Varsinaiset julkisuusperiaatteen alkuaskeleet nähtiin Ruotsi-Suomessa vuoden 1766 painovapausasetuksen myötä. Tämä voitiin nähdä erityisesti asiakirjajulkisuuden varhaisimpana muotona, sillä painovapauden toteutuminen edellytti tietynasteista asiakirjajulkisuutta. Pääperiaatteena pidettiin sitä, että painovapauden rajoituksista säädettäisiin tarkemmin asetuksessa. Tätä voidaan pitää hyvin tyypillisenä sääntelymallina, joka on käytössä tietyin lisäedellytyksin myös perusoikeuksien osalta vielä nykyäänkin.[80] Merkittävä kehitysaskel nähtiin vuoden 1865 painovapausasetuksen myötä, kun kansalaisille taattiin oikeus julkaista ja painattaa informaatiota sekä näitä oikeuksia varten saada tietoa esivallan antamista virallisista ilmoituksista, asetuksista ja muista julkisista asiakirjoista.[81]

Itsenäisen Suomen hallitusmuodon 10 §:n painovapautta koskevalla säännöksellä pyrittiin varmistamaan ennakkovalvonnankielto. Tarkemmin säädettiin myös oikeudesta painaa yleisiä asiakirjoja. Lopulta vaiheikkaan valmisteluprosessin myötä Suomessa aikaansaatiin vuonna 1952 voimaan tul-

[77] Korhonen 2003, s. 36—37.
[78] Konstari 1977, s. 17—20.
[79] Korhonen 2003, s. 39.
[80] Ibid. s. 40—42. Tosin nykyisin edellytetään lakitasoista sääntelyä näissä tilanteissa.
[81] Mäenpää 2016, s. 1—5 ja Korhonen 2003, s. 43.

lut laki yleisten asiakirjain julkisuudesta. Kyseisessä laissa tunnustettiin kiistatta julkisuusperiaatteen olemassaolo ja sen keskeinen asema demokraattisessa yhteiskunnassa. Myös painovapauden ja asiakirjajulkisuuden nähtiin eriytyvän toisistaan tämän lain myötä.[82]

Julkisuusperiaatetta pidetään nykyisin monessa Euroopan valtiossa perusoikeutena myös Pohjoismaiden ulkopuolella.[83] Euroopan neuvosto on antanut vuonna 1982 julistuksen ilmaisunvapaudesta, jonka tavoitteena oli asettaa julkiselle sektorille velvoite noudattaa avointa informaatiopolitiikkaa. Tämän lisäksi Euroopan neuvosto on julkaissut lukuisia suosituksia julkisuuden lisäämiseksi, muun muassa antamalla suosituksen viranomaistietojen julkisuudesta. Erityisesti tietosuoja- ja julkisuusperiaatteen välisen perusoikeuspunninnan kannalta merkittävänä voidaan pitää vuonna 1991 hyväksyttyä viranomaisten hallussa olevien henkilötietojen julkisuutta koskevaa suositusta. Sen mukaan oikeus saada tietoja viranomaisen julkisista asiakirjoista ei merkitse sitä, ettei julkisten tietojen käytössä ja rekisteröinnissä noudatettaisi tietosuojalainsäädännöstä johtuvia periaatteita.[84]

Eurooppaoikeudessa vuoden 1992 Maastrichtin sopimuksen[85] päätösasiakirjaan liitettiin julistus n:o 17, jossa todettiin avoimuuden vahvistavan toimielinten kansanvaltaisuutta sekä luottamusta hallintoa kohtaan. Lisäksi Euroopan unionin sekundaarioikeuden tasolla oli jo varhaisessa vaiheessa säännöksiä yksilön tiedonsaantioikeuksista[86]. Sittemmin julkisuusperiaatetta on käsitelty lukuisissa unionin toimielinkohtaisissa käytännesäännöissä ja päätöksissä.[87]

Nykyisin julkisuusperiaatetta ilmentävät monet Euroopan unionin sekundaarioikeudelliset sekä primaarioikeudelliset instrumentit, kuten Euroopan unionin perustamissopimuksissa olevat maininnat tiedonsaantioikeuksista sekä avoimuudesta.[88] Perusoikeuskirjan 41 artiklan säännöksen voidaan myös nähdä vahvistaneen julkisuusperiaatetta yhtenä eurooppaoikeudellisena perus- ja ihmisoikeutena. Sen 41 artiklan nojalla julkisuuden elementteinä voidaan nähdä henkilön oikeus tutustua itseään koskeviin asiakirjoihin, puolustautumisoikeuksiin liittyvä oikeus tutustua asiaansa koskeviin asiakirjoihin[89], oikeus tutustua asiaansa välillisesti koskeviin asiakirjoihin sekä jokaisen oikeus tutustua asiakirjoihin yleisöjulkisuuden nojalla.[90] Myös Euroopan ihmisoikeussopimuksessa on maininta julkisuusperiaatteesta, jonka mukaan kyse on oikeudesta julkiseen tietoon.[91]

---

[82] Konstari 1977, s. 76—84 yleisten asiakirjain julkisuudesta annetusta laista (83/1951).
[83] Korhonen 2003, s. 46.
[84] Mäenpää 2016 s. 25—28 ja Korhonen 2003, s. 48.
[85] Tunnetaan myös nimellä sopimus Euroopan unionista (SEU).
[86] Huomaa esim. 1.2.1983 annettu neuvoston asetus ETY, Euratom N:o 354/83 (*arkistoasetus*), jonka mukaan sellaista asiakirjaa ei saa julkaista, jonka salassapitoa ei ole kumottu.
[87] Korhonen 2003, s. 50.
[88] Ibid. s. 51.
[89] Lähinnä kuulemisoikeuteen liittyen.
[90] Kuusikko 2001, s. 431—434.
[91] Mäenpää 2016, s. 24—25 ja Korhonen 2003, s. 63; Huomaa myös Euroopan ihmisoikeussopimuksen sananvapautta käsittelevän 10 artiklan merkitys siihen sisältyvänä oikeutena hankkia tietoa; Eurooppaoikeudellisessa

Johtopäätöksenä voidaan todeta, että julkisuusperiaatteella on keskeinen rooli tiedonvälityksen ja sananvapauden toteuttamisessa.[92] Kyse on kansalaisten vaikutusmahdollisuuksien takaamisesta. Näin ollen julkisuusperiaatteen sääntelyllä on vaikutusta pelkkää asiakirjajulkisuutta laajemminkin tiedon sääntelyyn viranomaistoiminnassa. Tämä ilmenee henkilötietojen käsittelyn kontekstissa myös julkisuuslain 28 §:ssä, jonka mukaan *"oikeus saada tieto ja muuhun henkilötietojen luovuttamiseen viranomaisen henkilörekisteristä sovelletaan, mitä viranomaisten toiminnan julkisuudesta säädetään"*. Julkisuusperiaatteella on myös läheinen yhteys median mahdollisuuksiin levittää tietoa sekä median vapauteen.[93] Laajemmassa kuvassa julkisuusperiaate on hallinnon avoimuuden takaava perustavanlaatuinen oikeusperiaate ja näin ollen se on otettava huomioon myös henkilötietojen suojaa sekä henkilötietojen käsittelyn asianmukaisuutta arvioitaessa.[94]

## 2. Perus- ja ihmisoikeuksien vaikutus henkilötietojen käsittelyyn

Sitä, mitä yksityisyys tarkoittaa ja mikä on yksityisyyden suojan laajuus, on hankala tarkastella pelkästään kansainvälisten ihmisoikeussopimusten näkökulmasta. Yhdistyneiden kansakuntien (YK) erityisraportoija on todennut oikeutta yksityisyyteen käsittelevässä raportissaan, että hänen roolinsa on erityisesti lisätä tietoisuutta yksityisyyttä koskevista kysymyksistä. Vuonna 2016 antamassaan raportissa YK:n ihmisoikeusneuvostolle hän totesi, että yksityisyyden käsite tunnustetaan kaikissa yhteiskunnissa ja kulttuureissa sekä niiden historiassa, mutta yksityisyyden määritelmää ei ole sitovasti ja yleisesti hyväksytty globaalilla tasolla. Itse asiassa YK:n kansalaisoikeuksia ja poliittisia oikeuksia koskeva yleissopimus (*KP-sopimus*, SopS 8/1976) ei sisällä yksiselitteistä määritelmää yksityisyydelle, vaan se käytännössä estää ainoastaan mielivaltaisen ja laittoman puuttumisen yksilön erikseen määrittelemättömään yksityisyyteen.[95]

### 2.1. Kansainväliset sopimukset

Yhteiskuntien globalisoituminen ja kehittyminen verkkoyhteiskunniksi on luonut painetta säännellä ylikansallisesti henkilötietojen käsittelyä ja tietosuojaa. Erityisesti yksityinen sektori on lobannut erinäisiä hankkeita[96], jotta regulaatio olisi yhtenäisempää ja mahdollistaisi entistä tehokkaammin tietojen siirtämisen valtiosta toiseen ilman, että eri valtioiden lainsäädännölliset erot aiheuttaisivat kohtuuttoman suuria esteitä tälle, muun muassa lainsäädännöllisistä eroavaisuuksista johtuen. On myös huomattava, että internet on globaalin tietojenkäsittelyn mahdollistava fasiliteetti, johon on

kontekstissa tulee huomioida myös se, mitä säädetään EU:n julkisuusasetuksessa (EY) N:o 1049/2001 EU:n toimielinten, elinten ja laitosten asiakirjojen julkisuudesta.

[92] Mäenpää 2016, s. 3—5 ja Kulla — Koillinen 2014, s. 1.

[93] Tiilikka 2008, s. 42 ja Olli Mäenpään lausunto perustuslakivaliokunnalle, 6.2.2019, s. 1.

[94] Mäenpää 2008, s. 82.

[95] Data Protection for Human Rights Defenders, 2018, s. 38—39.

[96] Lobbaamisen merkitys on nähtävissä myös GDPR:n säätämisprosessissa, jossa esimerkiksi Googlen omistava Alphabet Inc., monen muun toimijan ohella, pyrki laajasti vaikuttamaan yhtenäisen tietosuojalainsäädännön sisältöön harmonisoimisen edistämiseksi.

pääsy kaikkialta maailmasta. Tämän takia myös henkilötiedot ovat yhä helpommin siirrettävissä valtioista toiseen sekä saatavilla eri valtioista käsin. Erinäisissä sosiaalisen median palveluissa kerätäänkin henkilötietoja samanaikaisesti usean eri valtion kansalaisista tai asukkaista ja ne ovat nähtävillä globaalisti ympäri maailmaa.[97]

Vuonna 1980 julkaistu OECD:n tietosuojasuositus ei ole sitova valtiosopimus, mutta ansaitsee tulla mainituksi tässä yhteydessä yhtenä ensimmäisistä ylikansallisista henkilötietojen suojaa koskevista lainsäädäntösuosituksista. Suosituksessa kiinnitettiin huomiota erityisesti valtioiden rajat ylittävään henkilötietojen siirtämiseen sekä tällaisissa tilanteissa tapahtuvaan tietojen keräämiseen. Henkilötietojen suojan kunnioittamisen varmistaminen periaateluontoisilla kansainvälistä tiedonsiirtoa koskevilla yleisperiaatteilla ilmentää myös hyvin myöhemmin yleistynyttä trendiä säännellä tietosuojasta nimenomaan periaateluontoisesti.[98]

Euroopan neuvosto on aikaisemmin mainitun vuoden 1981 tietosuojasopimuksen jälkeen korostanut tietosuojan ihmisoikeustasoista luonnetta. Tietosuojasopimus oli itsessään yleissopimus, jonka tarkoituksena oli suojata yksilöitä automaattisen tietojenkäsittelyn kontekstissa. Kyseinen sopimus on kuitenkin syytä mainita tässä yhteydessä, sillä kansainvälisen oikeuden näkökulmasta kyse oli sitovasta instrumentista, vaikka se ei vielä asettanutkaan tietosuojaa ihmisoikeuksien tasolle. Suomessa tietosuojasopimus tuli voimaan vuonna 1992 (SopS 36/1992). Euroopan neuvosto on lisäksi monilla ei-sitovilla instrumenteilla pyrkinyt kehittämään hyvän tietojenkäsittelyn kulttuuria muun muassa suoramarkkinointia, poliisitoimea, sosiaaliturvaa ja työelämän tietosuojaa koskevilla suosituksillaan.[99]

Euroopan ihmisoikeussopimus on kansainvälisoikeudellisesti sitova ihmisoikeuksia ja perusvapauksia suojaava yleissopimus.[100] Sen 8 artiklassa[101] säädetään oikeudesta nauttia yksityis- ja perhe-elämän kunnioittamisesta:

1. *”Jokaisella on oikeus nauttia yksityis- ja perhe-elämäänsä, kotiinsa ja kirjeenvaihtoonsa kohdistuvaa kunnioitusta.*
2. *Viranomaiset eivät saa puuttua tämän oikeuden käyttämiseen, paitsi kun laki sen sallii ja se on välttämätöntä demokraattisessa yhteiskunnassa kansallisen ja yleisen turvallisuuden*

[97] Bygrave 2002, s. 257.
[98] Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of the Personal Data, 23.9.1980.
[99] Ks. esim. Suoramarkkinointia koskeva suositus R(85) 20/25.10.1985, Sosiaaliturvan tietosuojaa koskeva suositus R(86) 1/23.1986, Poliisitoimen tietosuojaa koskeva suositus R(87) 15/17.9.1987, Työelämää koskeva suositus R(89) 2/18.1.1989 ja Henkilötietojen suojaamisesta maksutapahtumissa annettu suositus R(90) 19/13.9.1990.
[100] Kuten todettu, EIS annettiin vuonna 1950 ja Suomi liittyi siihen vuonna 1989.
[101] EIS 8 artiklan yksityis- ja perhe-elämän suojaa koskeva säännös sisältyi myös alkuperäiseen vuonna 1950 annettuun Euroopan ihmisoikeussopimukseen.

*tai maan taloudellisen hyvinvoinnin vuoksi, tai epäjärjestyksen tai rikollisuuden estämiseksi, terveyden tai moraalin suojelemiseksi, tai muiden henkilöiden oikeuksien ja vapauksien turvaamiseksi."*

Säännöksen 1 kohdassa säädetään yksityisyyden suojasta sekä horisontaalisessa että verikaalisessa suhteessa. Sen 2 kohdassa puolestaan tuodaan esille, että yksityisyyttä on mahdollista rajoittaa lähinnä vertikaalisessa suhteessa yleiseen etuun perustuen. Euroopan ihmisoikeussopimus ei EU:n perusoikeuskirjasta poiketen kuitenkaan sisällä erillistä henkilötietojen suojaa koskevaa ihmisoikeutta, vaan sen on katsottu sisältyvän yksityisyyteen Euroopan ihmisoikeustuomioistuimen (EIT) oikeuskäytännössä. Lisäksi perusoikeuskirjassa edellytetään jäsenvaltioiden asettavan riippumattoman viranomaisen valvomaan tietosuojan toteutumista lisäedellytyksenä Euroopan ihmisoikeussopimukseen nähden.

Vuonna 1997 Euroopan ihmisoikeustuomioistuin totesi ratkaisussaan Z. v. Suomi, että henkilötietojen suoja on perus- ja ihmisoikeustasoinen oikeus, jonka avulla yksilö voi nauttia oikeudestaan hänen yksityis- ja perhe-elämäänsä koskevaan kunnioitukseen.[102] Vuonna 2008 Euroopan ihmisoikeustuomioistuin totesi ratkaisussa Biriuk v. Liettua, että HIV-positiivisen henkilön terveystietojen julkaisemisessa oli kyse selkeästi sellaisesta yksilön vapauksiin puuttumisesta, joka on perus- ja ihmisoikeusnäkökulmasta, ja erityisesti yksityisyyttä koskevan oikeuden nojalla, kielletty.[103] Aikaisemmin vuonna 2000 Euroopan ihmisoikeustuomioistuin oli puolestaan todennut ratkaisussa Rotaru v. Romania, että virheellisten henkilötietojen levittämisessä oli kyse yksityisyyden loukkaamisesta ja rekisterinpitäjän olisi tullut sallia yksilölle pääsy omiin henkilötietoihinsa sekä sallia niiden oikaiseminen taikka tietojen poistamista koskeva pyyntö[104].[105]

Yksityisyyden ja tietosuojan kansainvälistä ihmisoikeusluonnetta kuvaa se, että kyseisestä oikeudesta säädetään globaalien valtiosopimusten ohella myös lukuisissa alueellisissa ihmisoikeusinstrumenteissa. Tästä esimerkkinä voidaan nostaa esille vuonna 2012 Kaakkois-Aasian maiden järjestön (ASEAN) antama ihmisoikeusjulistus, joka sisältää maininnan ihmisoikeustasoisesta oikeudesta tietosuojaan yksityiselämän suojan ohella. Julistuksessa todetaan, että jokaisella yksilöllä on oikeus vapauteen mielivaltaiselta yksityisyyteen, perhe-elämään, kotiin tai kirjeenvaihtoon, mukaan lukien henkilötietoihin, puuttumiselta.[106] Vaikka kyseisessä ihmisoikeusjulistuksessa henkilötietoihin puuttuminen mainitaan erikseen, on kuitenkin huomattava, että ASEAN:n ihmisoikeusjulistuksessa tietosuoja nähdään edelleen yksityisyyteen kuuluvana elementtinä.

[102] EIT: Z. v. Suomi, 25.2.1997.
[103] EIT: Biriuk v. Liettua, 25.2.2009.
[104] EIT: Rotaru v. Romania, 4.5.2000.
[105] Data Protection for Human Rights Defenders, 2018, s. 42—43.
[106] Ibid. s. 44.

Vuonna 1988 YK:n ihmisoikeuskomitea totesi KP-sopimuksen 17 artiklassa[107] sekä ihmisoikeuksia koskevan yleismaailmallisen julistuksen 12 artiklassa säädettyä oikeutta yksityisyyteen koskevassa yleisessä lausunnossaan[108], että henkilötietojen säilyttämisen tietokoneella, tietopankissa tai muussa lähteessä, on sitten kyse yksityisen tai julkisen sektorin toimijasta, täytyy olla säänneltyä lain tasolla. Nykyisin myös Suomen perustuslain 10.1 §:ssä todetaan, että henkilötietojen suojasta säädetään tarkemmin lailla, jolloin sen rajoittaminen on mahdollista ainoastaan tarkkarajaisella ja soveltamisalaltaan selkeällä lailla, joka ei puutu perusoikeuden ydinsisältöön.

Yksityisyydellä ja tietosuojalla on kiinnekohtia myös moniin muihin perus- ja ihmisoikeustasoisiin oikeuksiin ja vapauksiin. Näistä voidaan mainita erityisesti oikeus syrjimättömyyteen, josta on säädetty KP-sopimuksen sekä ihmisoikeuksia koskevan yleismaailmallisen julistuksen (UDHR, engl. *Universal Declaration of Human Rights*) 7 artiklassa samoin kuin monissa alueellisissa ihmisoikeusinstrumenteissa. Suomenkielisenä ilmaisuna on ehkä luonnollisempaa käyttää tässä yhteydessä yhdenvertaisuuden käsitettä. Tietoja yksilön henkilökohtaisista ominaisuuksista voi paljastua joko suoraan tai välillisesti ja näiden tietojen joukossa saattaa olla myös sellaista sisältöä, jota hän ei välttämättä halua muiden tietoon ja joita voidaan käyttää syrjivällä tavalla. Erityisesti yksityisyyteen ja tietosuojaan liittyvänä elementtinä, oikeus olla paljastamatta näkymättömiä itseään koskevia piirteitä, kuten uskontoa, seksuaalista suuntautumista, sukupuoli-identiteettiä tai terveydentilaa, voi olla perustana myös syrjinnän riskin torjumiseksi. Vahva tietosuoja siis varmistaa, että yksilö hallitsee edelleen tietojaan, jotka voivat johtaa syrjintään silloinkin, kun tiedot ovat jo jonkin kolmannen osapuolen hallussa.[109]

Näin ollen voidaankin todeta, että luvaton pääsy toisen henkilötietoihin voi yksityisyyden suojan ja tietoturvaloukkauksen lisäksi johtaa syrjintään. Kyse ei kuitenkaan ole pelkästään luvattoman pääsyn aiheuttamista riskeistä, vaan myös muunlaisista luvattomista käsittelytoimista, kuten rekisteröityjen profiloimisesta tämän henkilötietojen perusteella syrjiviä tarkoitusperiä varten. Valtion toimijat ja yksityiset yritykset voivat käyttää profilointia osana päätöksentekoaan, joka vaikuttaa siihen, miten henkilöitä kohdellaan, mitä palveluita heille pidetään tarjolla sekä millä ehdoin. Tämän takia on olemassa vaara, että henkilö kohtaa syrjintää, jos profiloinnin seurauksena hän saa epäsuotuisamman kohtelun johtuen erityisominaisuudesta, mitä ei voida neutraalisti perustella. Näin käy erityisesti, mikäli profilointiin käytetään algoritmeja, jotka kehittävät itse itseään, siis tekoälyä hyödynnettäessä, ja tällaiset algoritmit tiedostamatta oppivat uusia käytäntöjä harhaoppien kautta. Yksi esimerkki edellä mainitusta on yhdysvaltalainen riskiarviointiprosessi, jossa arvioidaan, pitäisikö

---

[107] KP-sopimuksen 17 artikla: "*1. Kenenkään yksityiselämään, perheeseen, kotiin tai kirjeenvaihtoon ei saa mielivaltaisesti tai laittomasti puuttua eikä suorittaa hänen kunniaansa ja mainettaan loukkaavia hyökkäyksiä. 2. Jokaisella on oikeus lain suojaan tällaista puuttumista tai tällaisia hyökkäyksiä vastaan*."

[108] "*General comment*".

[109] Data Protection for Human Rights Defenders, 2018, s. 46—48.

rikoksesta syytetty henkilö vapauttaa takuita vastaan. Algoritmit käyttivät poliisin hallussa olevia tietoja, kuten ihmisten pidätysten lukumäärää samasta rikoksesta, riskiarvioinnin pohjana. Koska poliisin pidätykset ovat saattaneet johtua rodullisesta syrjinnästä, algoritmit ovat johtaneet siihen, että tietyt etniset vähemmistöt vapautetaan takuita vastaan harvemmin kuin toiset. Tämän takia muun muassa GDPR sisältää erityissääntelyä, joka koskee nimenomaisesti profilointia ja automatisoitua päätöksentekoa.[110]

Oikeus sananvapauteen on toinen olennaisesti yksityisyyteen ja tietosuojaan vaikuttava perus- ja ihmisoikeus, josta säädetään YK:n ihmisoikeuksia koskevan yleismaailmallisen julistuksen sekä KP-sopimuksen 19 artiklassa ja lisäksi useissa alueellisissa ihmisoikeusinstrumenteissa. Kyseinen ihmisoikeus sisältää vapauden etsiä, vastaanottaa ja levittää tietoja, ideoita ja mielipiteitä alueellisista rajoista riippumatta ja missä tahansa muodossa. Kyky pysyä nimettömänä eli anonyyminä mielipiteenilmaisussa on ollut useissa viimeaikaisissa tapauksissa kriittisen tarkastelun kohteena. Sellaisissa yhteiskunnissa, joissa mielipiteen ilmaiseminen voi johtaa kostoon tai vainoon, yksilöt voivat monesti kertoa käsityksensä asioista ainoastaan anonyyminä, minkä erityisesti internet mahdollistaa. Eri puolilla maailmaa tätä ihmisen kykyä pysyä anonyyminä pyritään heikentämään. Ainakin 49 Afrikan valtiota vaativat nykyisin yksilöä rekisteröimään henkilökohtaiset tietonsa verkkopalvelun tarjoajien järjestelmiin ennen SIM-kortin aktivoimista, mikä johtaa laajojen käyttäjätietoja sisältävien tietokantojen luomiseen ja estää ihmisiä toimimasta tosiasiallisesti anonyymisti internetissä ainakin suhteessa valtionhallintoon. Tämä on aivan olennainen ilmentymä siitä, miksi tietosuojaa on pidettävä niin perustavanlaatuisena oikeutena verkkoyhteiskunnassa myös muiden perus- ja ihmisoikeuksien toteutumisen kannalta. Täytyy muistaa, että nimenomaan sananvapauden isänä pidetty Voltairekin käytti aikoinaan sananvapautta anonyymisti.[111]

Yhteenvetona voidaankin todeta, että on olemassa neljä keskeistä tekijää, jotka määrittävät, onko valtiossa ihmisoikeuksia kunnioittava tietosuojan taso. Ensinnäkin valtiolla on oltava oma tietosuojalaki ja tähän tietosuojalakiin on sisällytettävä kansallisesti sovitut tietosuojavaatimukset. Lisäksi tietosuojan on oltava riittävän kattavaa ja valtiolla on oltava oma täytäntöönpano- tai sääntelyviranomainen, joka antaa lausuntoja ja suosituksia sekä valvoo kansallisen tietosuojan tilaa riippumattomasti.[112] Ensimmäiset kaksi toimintavelvoitetta perustuvat jo nykyisiin ihmisoikeussopimuksiin.

On huomattava, että valtioon kohdistetaan ihmisoikeussopimuksien täytäntöönpanossa sekä negatiivisia että positiivisia velvoitteita. Negatiivisella velvoitteella tarkoitetaan velvoitetta pidättäytyä toimista, jotka vaikuttavat haitallisesti ihmisoikeuksien toteutumiseen. Positiiviset velvoitteet edel-

[110] Data Protection for Human Rights Defenders, 2018, s. 46—48.
[111] Ibid. s. 47—48.
[112] Ibid. s. 52—53.

lyttävät valtiota ryhtymään toimenpiteisiin ihmisten suojelemiseksi. Kuten edellä on todettu, tietosuojasta on säädettävä YK:n kannanottojen perusteella lakitasoisesti ja lisäksi on todettu, että tietojen käsittely voi aiheuttaa riskin yksilön perus- ja ihmisoikeuksien toteutumiselle, erityisesti oikeudelle yksityisyyteen. Ihmisoikeuskomitea on lisäksi tullut siihen johtopäätökseen, että lainsäädännössä on määriteltävä, kenellä on pääsy henkilön yksityiselämää koskeviin tietoihin sekä miten niitä voidaan käsitellä ja hyödyntää. Se, että tietosuojasääntely on riittävän kattavaa ja että valtioilla on oma tietosuojaviranomainen, on puolestaan varmistettu Euroopassa unionin lainsäädännön toimesta.[113]

### 2.2. Kansallinen perusoikeussääntely

Ruotsi on ollut ensimmäinen yleisen tietosuojalain käyttöön ottanut valtio (*datalag*) vuonna 1973. Tässä yhteydessä voidaan puhua ensimmäisen sukupolven tietosuojalainsäädännöstä. Ajatuksena oli tällöin vastata tietojenkäsittelyn tietokoneistamisen asettamiin haasteisiin ja kysymyksiin muun muassa siitä, pitäisikö tietojenkäsittelytoiminnan olla itseasiassa luvanvaraista.[114] Suomen tietosuojalainsäädännön kehityksessä ruotsalainen tietosuojalainsäädäntö on toiminut monelta osin esikuvana Pohjoismaiden neuvostossa käytyjen keskustelujen myötä. Niinpä vuonna 1987 Suomen eduskunta lopulta hyväksyi henkilörekisterilain. Kyseessä oli Ruotsin tietosuojalain tapaan yleislaki, joka oli tarkoitettu sovellettavaksi ainoastaan silloin kun muissa laeissa ei ollut tarkempia säännöksiä tietojenkäsittelystä. Säädös ilmensi myös aikaisemmin todettua tietosuojalainsäädännöllistä sääntelytarkkuutta koskevaa havaintoa siitä, että tietosuojalainsäädäntö on ollut vanhastaan hyvin periaateluontoista. Henkilörekisterilaissa omaksuttiin rekisterinpidon itsestäänselvyyden periaate sekä hyvä rekisterinpitotapa.[115]

Kansallisella tasolla henkilötietojen suojasta tuli perusoikeus vasta Suomen perusoikeusuudistuksen ja unionin henkilötietodirektiivin myötä.[116] Vuoden 1995 perusoikeusuudistuksessa Suomen hallitusmuodon 8 §:ään lisättiin säännös yksityiselämän suojasta, jonka yhteydessä todettiin, että henkilötietojen suojasta säädetään tarkemmin lailla. Suomen perustuslaki tuli voimaan 1.3.2000 ja käytännössä HM:n 8 § siirrettiin sellaisenaan uuteen perustuslakiin. Näin ollen säännöstä tulkitessa on aiheellista huomioida myös vuoden 1995 perusoikeusuudistuksen pohjana ollut hallituksen esitys ja muu valmisteluaineisto hallitusmuodon 8 §:ään liittyen.

Perustuslain 10.1 §:ssä todetaan, että ”*jokaisen yksityiselämä, kunnia ja kotirauha on turvattu. Henkilötietojen suojasta säädetään tarkemmin lailla”.* Hallituksen esityksessä vuoden 1995 perusoi-

[113] Data Protection for Human Rights Defenders, 2018, s. 54—57.
[114] Saarenpää 2012, s. 328 ja Wallin 1991, s. 7 Ruotsin ensimmäisestä tietosuojalaista.
[115] Neuvonen 2014, s. 31—32 ja Saarenpää 2012, s. 328.
[116] Alapuranen et al. 2005, s. 19.

keusuudistuksesta omaksutun termin ”*jokainen*” osalta todettiin sen tarkoittavan kaikkia luonnollisia henkilöitä eli nimenomaisesti ihmisyksilöitä. Yleisesti perusoikeusuudistuksessa todettiin, että kyse oli Suomen perusoikeusjärjestelmän saattamisesta vastaamaan kansainvälisissä ihmisoikeussopimuksissa asetettuja vaatimuksia ja erityisesti Euroopan ihmisoikeussopimusta.[117]

Kuten voidaan huomata, Suomen perustuslaki sisältää lainsäädäntötoimeksiannon, johon henkilötietolaki ja sittemmin tietosuojalaki sekä tietojenkäsittelyä koskeva erityislainsäädäntö on vastannut. Oikeusministeriö on todennut muun muassa perustuslakivaliokunnan lausuntoihin viitaten, että lakiviittauksilla voi olla itsenäistä oikeudellista merkitystä neljässä erityisessä suhteessa. Ensimmäiseksi, lakiviittaus voi johtaa siihen, että kyseinen asiakokonaisuus on pidätettävä lain alaan. Toiseksi, sillä voidaan valtuuttaa lainsäätäjä säätämään perustuslaista jossain määrin poikkeavaa lainsäädäntöä. Kolmanneksi, lakivarauksen sisältöön voi kuulua toimivaltaa rajoittavia säännöksiä ja viimeiseksi kyse voi olla puhtaasta lainsäätäjälle asetetusta toimeksiannosta. Tällöin lakiviittauksen huomioon ottaminen voi osoittaa, että laintulkinnassa on otettava huomioon tavallisen lainsäädännön muodostaman kokonaisuuden lisäksi perustuslain sisältö tavallista yksityiskohtaisemmalla tavalla.[118]

Hallituksen esityksessä on todettu, että ilmaisu ”lailla tarkemmin säädetään” viittaa siihen, että säännöksessä mainittu oikeus, kuten oikeus henkilötietojen suojaan, on pääsääntö. Lain on tarkoitus täsmentää säännöksen sisältöä, jolla ei kuitenkaan tarkoiteta pääsäännön perustan heikentämistä, vaan kyse on ennen kaikkea perustuslain säännöksen tarkentamisesta. Tällainen liikkumavara mahdollistaa joiltain osin perustuslain säännöksessä mainittua perusoikeutta rajoittavatkin säännökset toimeksiantoa täyttävässä tavallisessa lainsäädännössä.[119] Asia ei kuitenkaan täysin tyhjene edellä kuvattuun. On myös huomattava, että lakiviittauksen taustalla voi olla ajatus siitä, että perusoikeus todella edellyttää tuekseen tavallista lainsäädäntöä sen toteuttamiseksi tai vaihtoehtoisesti, perusoikeutta on mahdotonta kirjoittaa riittävän kattavaan tai ehdottomaan muotoon perustuslain tasolla. Tällaisen sääntelyvarauksessa kuvatun perusoikeuden tarkempi sisältö määrittyy vasta tavallisessa laissa. Ilmaisu ”tarkemmin” viittaakin siihen, että liikkumavaran käyttämisessä on kyse perustuslain ilmaisemaan pääsääntöön sidotusta lainsäädännöstä.[120]

On myös huomattava, että PL 22 §:n mukaan julkista valtaa käyttävillä tahoilla on velvollisuus aktiivisesti edistää perusoikeuksien toteutumista. Tämä julkiselle vallalle asetettu toimeksianto tarkoittaa muun ohella henkilötietojen suojan edistämistä. Hallituksen esityksessä todetaankin, että

[117] HE 309/1993 vp, s. 21-23 ja Saraviita 2011, s. 131.
[118] Oikeusministeriön julkaisu, 11/2006, s. 16—18.
[119] HE 309/1993 vp, s. 25—29.
[120] PeVM 25/1994 vp, s. 4—5.

lähtökohtana on vahvistaa julkisen vallan positiivista toimintavelvoitetta, jotta yksilön perusoikeudet tulevat huomioiduiksi kaikessa julkisessa vallankäytössä.[121] Kyse ei siis ole ainoastaan negatiivisesta vaikutuksesta, jonka mukaisesti julkinen valta pidättäytyy puuttumasta yksilön tärkeisiin oikeuksiin ja vapauksiin julkisen vallan ja yksityisen välisessä vertikaalisessa suhteessa. Kyse on pohjimmiltaan myös siitä, että perusoikeuksien on toteuduttava myös horisontaalisessa suhteessa muiden yksilöiden välillä aktiivisesti siitä huolehtimalla.[122]

Perustuslakiin asetetun tietosuojan myötä, perustuslakivaliokunnan asema erilaisten valtiollisten rekistereiden, kuten perusrekistereiden, arvioijana on kasvanut. Tietosuojan perusoikeusluonteesta johtuen esimerkiksi henkilötietojen säilytysajoista ei voida säätää ainoastaan asetuksen tasoisesti. Ainakin säilytysaikojen määräytymisen perusteista olisi säädettävä tavallisen lain tasoisesti, mikäli aikamääreiden säätäminen ei ole mahdollista. Lisäksi rekisteröidylle on turvattava riittävät oikeussuojakeinot häneen kohdistuvan käsittelyn yhteydessä, eikä läpinäkyvyyttäkään tietosuojaperiaatteena tule unohtaa. On huomattava, ettei läpinäkyvyys ole ainoastaan tietosuojaoikeudellinen periaate vaan kyse on myös laajemmasta hallinto-oikeudellisesta periaatteesta, jolla on läheinen yhteys aikaisemmin esitettyyn julkisuusperiaatteeseenkin.[123]

Yhteenvetona voidaankin todeta, että henkilötietojen suoja on kansallisella tasolla oma itsenäinen yksityisyydestä erillään oleva perusoikeus, jonka sisältö saa tarkemman merkityksensä tavallisesta laista. Laissa on mahdollista säätää rajoituksia henkilötietojen suojalle. Koska henkilötietojen suojasta on säädetty perustuslaissa samassa momentissa yksityisyyden suojan, kunnian ja kotirauhan kanssa, on selvää, että nämä näkökohdat on otettava huomioon tietosuojasta säädettäessä. Tietosuojalainsäädännön tulisikin olla myös yksilöiden yksityisyyden suojaa kunnioittavaa. Lisäksi on huomattava, että perustuslain tietosuojaa koskeva säännös ei aseta henkilötietojen suojaa millään tavalla erilaiseen asemaan yksityisessä tai julkisessa toiminnassa.[124]

On huomattava, että julkisuusperiaate perusoikeutena voi vaikuttaa hyväksyttävän tietosuojan tason arvioimiseen perusoikeuspunnintatilanteissa kyseisen periaatteen kohdistuessa julkisten organisaatioiden toimintaan sekä joissain yhteyksissä myös yksityisoikeudellisiin toimijoihin, erityisesti tekijänoikeuksiin liittyen. Tällöin julkisen vallan käyttämisen yksityistämistä ei ole nähtävissä mer-

[121] HE 309/1993 vp, s. 25—28.
[122] Tuori – Lavapuro et al. 2011, s. 809—815 ja Kauppi 2007, s. 246—247.
[123] Ks. esim. PeVL 11/2008 vp. lentomatkustajatietojen siirrosta lentoyhtiöltä viranomaisen käyttöön; PeVL 11/1997 vp. tietojen poistamisesta poliisin henkilörekisteristä; PeVL 7/1997 vp. televalvonnasta ja DNA-tunnisteiden tallentamisesta poliisin henkilörekisteriin.
[124] Saraviita 2011, s. 184—185.

kittävänä riski tietosuojalle. Itse asiassa tilanne on päinvastainen, sillä ilmiötä on pidetty ongelmallisena nimenomaan julkisuusperiaatteen kannalta, kun aikaisemmin julkisina pidettyjä asiakirjoja pyritään mahdollisesti salaamaan perustellen niiden olevan liikesalaisuuksia[125].

## 3. Euroopan unionin oikeudelliset instrumentit ja niiden suhde perus- ja ihmisoikeuksiin

Euroopan unionin perusoikeuskirjan unionin kansalaisten ja unionin alueella asuvien vapauksia koskevan II luvun 7 artiklan mukaan jokaisella on oikeus siihen, että hänen yksityis- ja perhe-elämäänsä, kotiaan sekä viestintäänsä kunnioitetaan. II luvun 8 artiklassa on varsinainen tietosuojaa perusoikeutena määrittävä säännös:

*”8 artikla Henkilötietojen suoja*

1. *Jokaisella on oikeus henkilötietojensa suojaan.*
2. *Tietojen käsittelyn on oltava asianmukaista ja sen on tapahduttava tiettyä tarkoitusta varten ja asianomaisen henkilön suostumuksella tai muun laissa säädetyn oikeuttavan perusteen nojalla. Jokaisella on oikeus tutustua niihin tietoihin, joita hänestä on kerätty, ja saada ne oikaistuksi.*
3. *Riippumaton viranomainen valvoo näiden säännösten noudattamista.”*

Yleinen tietosuoja-asetus nojaa EU:n perusoikeuskirjaan, jossa ensimmäistä kertaa kansainvälisellä tasolla vahvistettiin edellä kuvatusti tietosuojan olevan itsenäinen ja yksityisyydestä erotettavissa oleva perusoikeus.[126] Perusoikeutena tietosuoja sisältää kolme elementtiä. Ensinnäkin jokaisella on *oikeus henkilötietojen suojaan* ja toiseksi henkilötietojen asianmukaiseen käsittelyyn. Jotta perusoikeus tietosuojaan toteutuisi, on lisäksi jokaisella oikeus tutustua hänestä kerättyihin tietoihin ja saada ne oikaistuksi.[127]

Edellä mainittujen kolmen elementin nojalla oikeus henkilötietojen suojaan edellyttää, että henkilötietojen käsittelyn on oltava laadultaan asianmukaista ja tarkoitussidonnaista sekä käsittelylle on oltava laissa säädetty peruste ja lisäksi henkilötietojen suoja perusoikeutena luo rekisteröidylle kaksi oikeutta, oikeuden tulla unohdetuksi sekä oikaisuoikeuden.[128] Tämä on eräänlainen poikkeus pääsäännöstä, jonka mukaan yksinoikeuksia tietoon ei ole. Luonnollisilla henkilöillä on kuitenkin oikeus henkilötietoihinsa. Tietoon sekä muuhun aineettomaan kohdistuvat oikeudet ovat tyypillisesti kielto-oikeuksia eli ne antavat oikeudenhaltijalle mahdollisuudet kieltää muita hyödyntämästä informaatiota.[129] Toisin sanoen oikeudet tietoon ilmentyvät eri yhteyksissä hyvin samantyyppisin säännöksin. Immateriaalioikeuksien suojaa ei tule kuitenkaan sekoittaa henkilötietojen suojaan,

[125] Ks. esim. Heuru 2001, s. 212—213.
[126] Ks. esim. Wallin 2001, s. 374.
[127] Salokannel 2016, s. 536.
[128] Ollila 2014, s. 815.
[129] Pitkänen 2017, s. 583.

sillä immateriaalioikeuksien suojaamisessa on kyse lähinnä elinkeinovapaudesta, yksityisyyden suojasta tai omistusoikeudesta ja tiedonsaantioikeuksista.[130]

On huomattava, että tietosuojasta puhuttaessa kyse ei ole pelkästään tietojen suojaamisesta. Käsitteenä tietosuoja voi siis olla harhaanjohtava, sillä pohjimmiltaan kyse on tietosuojalainsäädännön avulla toteutettavasta yksilön suojelusta.[131] Kyse on siis luonnollisen henkilön sekä tämän perusoikeuksien suojaamisesta.[132] Saarenpään sanoin voidaan puhua sääntelystä, joka suojaa yksilöitä ja heidän perusoikeuksiaan henkilötietojen käsittelyn avulla toteutettavaa informaatioväkivaltaa vastaan.[133] Myös tietosuoja-asetuksen ensimmäisessä artiklassa todetaan, että kyseisellä asetuksella vahvistetaan säännöt luonnollisten henkilöiden suojelemiselle henkilötietojen käsittelyssä sekä suojellaan heidän perusoikeuksiaan ja -vapauksiaan sekä erityisesti heidän oikeuttaan henkilötietojen suojaan.

Perus- ja ihmisoikeudet ovat usein kuitenkin ristiriidassa toisiinsa nähden. Henkilötietojen suoja saattaa olla vastakkain esimerkiksi toiminnan- tai sananvapauden kanssa. Yksi havainnollistava esimerkki on KHO 1996-A-6, jossa todettiin, että CD-ROM-levykettä voidaan pitää tuotettuna kirjoituksena ja henkilörekisterilakia ei sovelleta, kun on kyse hallitusmuotoon perustuvasta painovapaudesta. Silloisen henkilörekisterilain tarkoituksena ei ollut puuttua hallitusmuodossa turvattuun sanan- ja painovapauteen.[134] Oikeus yksityiselämän suojaan tulikin perusoikeudeksi Suomessa aikaisemmin todetun mukaisesti vasta 1.8.1995 pitkälti EU-jäsenyyden myötä.[135]

On jo pitkään ollut selvää, että perusoikeutta voidaan rajoittaa toisella perusoikeudella. Näiden rajoitusten tulee kuitenkin olla perusoikeuksien kannalta hyväksyttäviä ja painavan yhteiskunnallisen tarpeen vaatimia. Lisäksi edellytetään, että rajoitukset ovat välttämättömiä asetettujen tavoitteiden saavuttamiseksi ja laajuudeltaan oikeassa suhteessa perusoikeuksien sekä yhteiskunnallisten intressien valossa, minkä perusteella perusoikeutta rajoitetaan. Rajoitukset eivät myöskään saa olla ristiriidassa Suomea ja laajemmin unionia[136] velvoittavien kansainvälisten ihmisoikeuksien kanssa.

---

[130] Saarenpää et al. 2016, s. 151.
[131] Saarenpää 2015, s. 324.
[132] Ibid. s. 324.
[133] Ibid. s. 324.
[134] HE 49 /1986 vp, s. 5 ja HE 311/1993 vp, s. 10.
[135] Tietosuojavaltuutetuntoimisto, 26.9.2013.
[136] Huomaa, että Lissabonin sopimuksen myötä EU:sta tuli oikeushenkilö, jolla on oma perusoikeuskirja (SEU:n 6 artiklan 1 kohta). Perusoikeuskirjan 8 artiklassa (2000/C 34/01) henkilötietojen suoja vahvistetaan perusoikeudeksi. Perusoikeuskirjan 7 artiklassa säädetään yksityis- ja perhe-elämän kunnioittamisesta. Kun Euroopan unionia voidaan pitää itsenäisenä oikeushenkilönä, voidaan myös nähdä, että Euroopan unionilla on itsenäinen velvollisuus toteuttaa ja turvata toiminnassaan sellaisia perus- ja ihmisoikeuksia, joihin EU on oikeushenkilönä sitoutunut. Niinpä Lissabonin sopimuksen myötä EU sitoutui Euroopan ihmisoikeussopimukseen (SEU:n 6 artiklan 3 kohta). Oikeus henkilötietojen suojaan on Euroopan ihmisoikeussopimuksen piirissä osana yksityisyyden suojaa sen 8 artiklassa. Näin ollen EU on toiminnassaan vastuussa perusoikeuskirjassa tunnustettujen perusoikeuksien toteuttamisen ohella myös Euroopan ihmisoikeussopimuksessa tunnustettujen ihmisoikeuksien toteuttamisesta.

Näin ollen tässäkin yhteydessä pidän perusteltuna tuoda esille myös kansainvälistä oikeutta arvioitaessa eurooppalaista yksityiselämän suojaa lähellä olevan henkilötietojen riittävän suojaamisen suhdetta muihin perusoikeuksiin unionin sääntelyn tasolla.[137]

Euroopan ihmisoikeustuomioistuin on tuonut havainnollistavasti esille sen, kuinka oikeus henkilötietojen suojaan kytkeytyy myös muihin ihmisoikeuksiin. Eräässä ratkaisussa oli kyse siitä, että kansalaiset olivat pyytäneet tuloksetta nähtävilleen heitä koskevia henkilötietoja henkilörekisteristä. Euroopan ihmisoikeustuomioistuin totesi, että Euroopan ihmisoikeussopimuksen 13 artiklan mukainen oikeus tehokkaaseen oikeussuojaan ei toteudu pelkästään sillä, että kansalaisilla on mahdollisuus kannella tietojen antamatta jättämisestä parlamentin oikeusasiamiehelle tai oikeuskanslerille.[138] Näin ollen tietosuoja-asetuksen 78 artiklassa painotetaan jokaisen oikeutta tehokkaisiin oikeussuojakeinoihin.

*Yksityiselämän suojalla* tarkoitetaan sitä, että ihmisellä tulee olla tietty rauhoitettu alue, johon kuuluvat asiat hänen tulee voida pitää omana tietonaan niin halutessaan.[139] Yksityiselämän suojan laajuus on yhteydessä myös henkilön yhteiskunnalliseen asemaan ja toiminnan laatuun sekä sen yhteiskunnalliseen merkitykseen.[140] Näin ollen asiakirjajulkisuus ei suoraan tarkoita sitä, että sen piiriin kuuluvat tiedot voitaisiin julkaista.[141] Tämä johtaa siihen, että asiakirjajulkisuuden alaan kuuluvia tietoja sisältävän henkilörekisterin on yhtä lailla täytettävä tietosuoja-asetuksen asettamat takeet henkilötietojen suojan täyttämisestä. Onkin todettu, että vaikka muun muassa sananvapaus on turvattu perustuslaissa, niin myös yksityiselämän suojalla on oma ydinalueensa, jota ei tule tehdä tyhjäksi toisen perusoikeuden tai -vapauden, esimerkiksi sananvapauden tai julkisuusperiaatteen, perusteella.[142]

---

[137] Ks. PeVM 25/1994 vp, s. 5.
Ks. myös esim. Pitkänen et al. 2013, s. 16, tulkitsi samansuuntaisesti.

[138] EIT: Segersted-Wiberg ja muut v. Ruotsi, 6.9.2006, kohdat 116 ja 117. Tehokkaiden oikeussuojakeinojen vaatimus johtaa toisin sanoen siihen, että unionin kansalaisella tai unionin alueella asuvalla tulisi näissä tapauksissa olla mahdollisuus valittaa asiasta tuomioistuimeen, jolloin pelkkä mahdollisuus kannella ylimmille laillisuusvalvojille ei ole riittävää. Tietosuojan osalta asian on toteutettu pitkälti mahdollisuudella valittaa rekisterinpitäjän toiminnasta riippumattomalle valvontaviranomaiselle ja sen päätöksestä hallintotuomioistuimiin.

[139] Heinonen et al. 2002, s. 913, Nuutila kuvasi yksityiselämää sanalla intimiteetti.

[140] HE 84/1974 vp, s. 3, vrt. myös rikoslain (39/1889) 24:8.3 ja 24:8.4 yksityiselämää loukkaavan tiedon levittämisestä: "*Yksityiselämää loukkaavana tiedon levittämisenä ei pidetä sellaisen yksityiselämää koskevan tiedon, vihjauksen tai kuvan esittämistä politiikassa, elinkeinoelämässä tai julkisessa virassa tai tehtävässä taikka näihin rinnastettavassa tehtävässä toimivasta, joka voi vaikuttaa tämän toiminnan arviointiin mainitussa tehtävässä, jos esittäminen on tarpeen yhteiskunnallisesti merkittävän asian käsittelemiseksi.*
*Yksityiselämää loukkaavana tiedon levittämisenä ei myöskään pidetä yleiseltä kannalta merkittävän asian käsittelemiseksi esitettyä ilmaisua, jos sen esittäminen, huomioon ottaen sen sisältö, toisten oikeudet ja muut olosuhteet, ei selvästi ylitä sitä, mitä voidaan pitää hyväksyttävänä.*"

[141] HE 184/1999 vp, s. 32.

[142] Hällström 2004, s. 3.

Toisaalta rekisterinpitäjällä on myös vastuu antamiensa tietojen oikeellisuudesta. Euroopan ihmisoikeustuomioistuin on todennut, että lehdistön tulee voida luottaa virallisiin raportteihin ja selvityksiin siinä suhteessa, että näiden sisältö on oikeellista, toimittajien tai muiden kansalaisten tarvitsematta erikseen tarkastaa esitettyjä väitteitä.[143] Niinpä on todettu, että henkilötietojen suoja pääsääntöisesti syrjäyttää julkisuusperiaatteen niissä tilanteissa, kun kysymys on henkilötietojen käsittelystä, jolloin ensisijaisesti suojataan ihmistä.[144] Tämä tulkinta on kuitenkin kritiikille altis, sillä myös julkisuusperiaatteella on oma ydinsisältönsä. Lisäksi kyseisessä tulkinnassa ei oteta riittävästi huomioon julkisuuslain 28 §:n viittaussäännöstä, jonka mukaan oikeuteen saada tietoa ja muuhun tietojen luovuttamiseen viranomaisen henkilörekisteristä sovelletaan julkisuuslakia. Näkemykseni mukaan henkilötietojen suojaan liittyvistä vaatimuksista voidaan poiketa julkisuuperiaatteen nojalla, mikäli kyse ei ole tietosuojan ja yksityisyyden ydin sisällöstä. Tällöin henkilötietojen julkisuuden on julkisuusperiaatteen nojalla oltava erityisen tärkeää.[145] Tämän takia myös yleisessä tietosuoja-asetuksessa on säädetty poikkeamisesta joistain tietosuojaperiaatteista, kun kyse on tietyistä yleisen edun nojalla ylläpidetyistä henkilörekistereistä.[146]

Tietyt henkilötiedot ovat kuitenkin erityisessä asemassa. Henkilötietolaissa näitä henkilötietoja on kutsuttu arkaluonteisiksi henkilötiedoiksi ja tietosuoja-asetuksessa sekä sen pohjalta säädetyssä tietosuojalaissa käytetään ilmaisua erityiset henkilötietoryhmät. Esimerkiksi yksilön terveyteen liittyvät tiedot kuuluvat tähän erityisten henkilötietojen ryhmään. Tällaisten tietojen käsittely edellyttää korostetusti sitä, ettei niiden käsitteleminen johda kansalaisten yksityisyyden suojan vaarantumiseen. Tämä näkemys pohjautuu Suomen perustuslakiin, EU:n perusoikeuskirjaan ja Euroopan ihmisoikeussopimukseen sekä tietosuojaan enemmän keskittyvään kansainväliseen Euroopan neuvoston yleissopimukseen (*Convention 108*).[147]

Perusoikeuksien suojaa tulee tarkastella suhteessa muihin perusoikeuksiin, mikä johtaa esimerkiksi terveystietojen osalta siihen, että huomioiduksi tulee myös EU:n perusoikeuskirjan 3 artiklan takaama jokaisen oikeus henkilökohtaiseen koskemattomuuteen. Tämä perusoikeus takaa lääketieteen sekä biologian alalla jokaiselle itsemääräämisoikeuden omaan kehoonsa. Tässä kohtaa itsemääräämisoikeudella tarkoitetaan henkilön vapaaehtoisuutta kyseisiin toimenpiteisiin. Vapaaehtoisuutta ei puolestaan voida saavuttaa ilman tietoista suostumusta, joka on hankittu laissa säädetyn

---

[143] EIT: Colombani, Incyan ja Le Monde v. Ranska, 25.6.2002.
[144] Saarenpää 2015, s. 331.
[145] Tähän tulkintaan viittaa myös se, mitä julkisuuslain 28 §:ssä säädetään viranomaisten henkilörekisterien julkisuudesta.
[146] GDPR:n 89 artikla. Huomaa myös EIS:n 8(2) artikla, jonka mukaan tietosuojasta voidaan poiketa vertikaalisessa suhteessa, kun kyse on yleisestä edusta. Säännöksen sanamuodon mukaan tietosuojasta poikkeaminen on mahdollista, kun se on nimenomaisesti demokraattisessa yhteiskunnassa välttämätöntä. Julkisuusperiaatteen on puolestaan nähty olevan yksi demokraattisen yhteiskunnan tunnusmerkeistä.
[147] Salokannel 2016, s. 534.
Ks. Convention for the protection of individuals with regard to automatic processing of personal data (1.10.1985).

menettelyn mukaisesti. Sama artikla kieltää lisäksi taloudellisen hyödyn tavoittelun ihmisruumiilla tai sen osilla. Lääketieteellisen tutkimuksen yhteydessä näitä perusoikeuksia joudutaan punnitsemaan perusoikeuskirjan 14 artiklassa taatun tieteen ja akateemisen tutkimuksen vapauden kanssa.[148]

### 3.1. GDPR ja sen suhde perus- ja ihmisoikeuksiin

Yleinen tietosuoja-asetus[149] on säädetty EU:n ja EU:n toiminnasta tehdyn sopimuksen (SEU ja SEUT, 2016/C 202/01) 16(2) artiklan nojalla. Sopimuksen mukaan EU:n parlamentti sekä neuvosto ovat toimivaltaisia antamaan luonnollisten henkilöiden suojaa koskevat säännöt, jotka koskevat tietosuojaa unionin alueella, silloin kun unionin toimielimet, elimet ja laitokset sekä jäsenvaltiot toteuttavat unionin soveltamisalaan kuuluvaa toimintaa. EU:n toimivalta ulottuu lisäksi henkilötietojen vapaata liikkuvuutta koskevaan sääntelyyn. Yleisen tietosuoja-asetuksen perusoikeusluonnetta tuo entisestään esille myös sen johdanto-osan 14 kappale, jonka mukaan asetus suojaa kaikkia luonnollisia henkilöitä asuinpaikasta sekä kansalaisuudesta riippumatta, kun kyse on henkilötietojen käsittelystä.[150] Seuraavaksi avaan sitä, miksi *suhteellisuus- ja subsidiariteettiperiaatteen* nojalla on nähty tarpeelliseksi säätää tietosuojasta nimenomaisesti asetuksella eikä direktiivillä, kuten aikaisemmin. Samassa yhteydessä käyn läpi GDPR:n sisältämien säännösten tarpeellisuutta suhteutettuna perus- ja ihmisoikeuksiin sekä aikaisempaan oikeuskäytäntöön ja -kirjallisuuteen.

Edellä todetusti, Euroopan perusoikeuskirjan 7 artiklan mukaan jokaisella on oikeus siihen, että hänen yksityis- ja perhe-elämäänsä sekä viestiensä luottamuksellisuutta kunnioitetaan. Lisäksi 8 artiklassa säädetään henkilötietojen suojasta. Henkilötietojen käsittelyn on tämän perusteella oltava asianmukaista ja tapahduttava tiettyä tarkoitusta varten joko asianomaisen henkilön suostumuksella[151] tai laissa säädetyn perusteen nojalla. Tähän sisältyy myös jokaisen perusoikeustasoinen oikeus saada tutustua hänestä kerättyihin tietoihin sekä oikeus saada oikaistuksi virheelliset tiedot. Riippumattomien viranomaisten tulee lisäksi valvoa tämän perusoikeuden noudattamista. Tietosuoja-asetuksen 31 artiklassa todetaankin, että rekisterinpitäjän ja henkilötietojen käsittelijän on

[148] Salokannel 2016, s. 536.

[149] GDPR:n 99 artiklan nojalla asetus tuli voimaan 24.5.2016 ja sitä alettiin soveltamaan 2 vuoden siirtymäajan jälkeen 25.5.2018.

[150] Salokannel 2016, s. 346.

[151] Huomaa, että kaikenlainen henkilötietojen käsittely ei ole sallittua edes rekisteröidyn suostumuksella. Henkilötietojen suojan perusoikeusluonnetta kuvaa hyvin se, että henkilön suostumuksellakin tapahtuvassa käsittelyssä on noudatettava pakottavaa tietosuojalainsäädäntöä. Havainnollistavia esimerkkejä löytyy myös tietosuojaoikeudellisesta erityislainsäädännöstä, kuten yksityisyydensuojasta työelämässä annetun lain (2004/759) 3 §, jonka mukaisesti työnantaja saa käsitellä vain välittömästi työsuhteen kannalta tarpeellisia työntekijän henkilötietoja eikä tarpeellisuusvaatimuksesta voida poiketa edes työntekijän suostumuksella. Lisäksi analogisena esimerkkinä voidaan todeta, että kaikenlainen lääketieteellinen tutkimuskaan ei ole sallittua edes tutkittavan suostumuksella, vaan siitä huolimatta on noudatettava tutkimuseettisiä säännöksiä sekä kunnioitettava yksilön oikeutta elämään, ja fyysistä koskemattomuuttakaan ei saa tarpeettoman epähumaaneilla tavoilla loukata edes tutkittavan suostumuksella.

pyynnöstä tehtävä valvontaviranomaisen kanssa yhteistyötä tämän valvontatehtävien suorittamiseksi. Tietosuoja-asetuksen 51(1) artiklan mukaan jäsenvaltion tulee asettaa valvontaviranomainen, joka on vastuussa kyseisen asetuksen soveltamisen valvonnasta perusoikeuksien ja -vapauksien suojaamisen takaamiseksi. Tietosuoja-asetuksen 55(1) artikla puolestaan edellyttää, että valvontaviranomaisilla on riittävät valtuudet tehtäviensä hoitamiseksi. Näin asetuksella on pyritty huolehtimaan siitä, että edellä mainittujen perusoikeuksien toteutumiselle on riittävät takeet.

EU:n sekä kansallisten toimielinten on noudatettava Euroopan perusoikeuskirjaa kaikessa toiminnassaan.[152] Unionin tuomioistuin on havainnut, että on tarvetta tehdä lainsäädäntöä koskevia tarkastuksia sen varmistamiseksi, että lainsäädäntö on perusoikeuskirjan mukaista.[153] Euroopan unionin tuomioistuin on todennut, että tietojen säilyttämistä koskeva direktiivi on pätemätön sen rikkoessa perusoikeuskirjan 7 ja 8 artikloissa säädettyjä yksityiselämän kunnioittamista sekä henkilötietojen suojaan koskevia perusoikeuksia.[154] Lisäksi tuotiin esille, että perusoikeuksien suojelun takeet on sisällytettävä EU:n lainsäädäntöön eikä niitä näin ollen tule jättää kansallisen lainsäätäjän harkintavallan varaan, sillä unioni on oikeushenkilönä myös itse vastuussa sellaisten perus- ja ihmisoikeuksien toteuttamisesta, mihin EU on sitoutunut.

Esille on nostettu voimakkaasti myös velvollisuus huomioida, mitä perusoikeuskirjassa säädetään, kun toimet vaikuttavat yksityiselämää, yksityisyyttä ja henkilötietojen suojaa koskevaan oikeuteen.[155] Edellä mainitun takia on perusteltua, että EU on pyrkinyt nykyistä tarkemmin sääntelemään myös niitä takeita, joiden johdosta voidaan katsoa henkilötietojen käsittelyn tapahtuvan perusoikeuskirjassa ja Euroopan ihmisoikeussopimuksessa säädettyjen perus- ja ihmisoikeuksien mukaisesti. Tästä syystä on säädetty yleinen tietosuoja-asetus, joka on jäsenvaltioissa suoraan sovellettavaa oikeutta rajallisine liikkumavaroineen.

Euroopan unionista tehty sopimus määrittelee sen 21 artiklassa unionin ulkoista toimintaa. Kyseisessä säännöksessä tuodaan esille, että myös kolmansien valtioiden kanssa tehtävässä yhteistyössä, kuten kauppasopimuksissa, ihmisoikeudet ovat olennainen tekijä osapuolten välisessä suhteessa. Kun digitaalinen vallankumous on luonut yhteiskunnalle, kansalaisille sekä liiketoiminnalle monia uusia mahdollisuuksia, on se herättänyt myös huolta perus- ja ihmisoikeuksien tehokkaasta suojelemisesta digitalisoituneessa yhteiskunnassa erityisesti, kun henkilötietojen kaupalliset hyödyntämismahdollisuudet ovat moninaistuneet entisestään.[156]

---

[152] EU:n perusoikeuskirjan soveltamista koskeva kertomus vuodesta 2014, s. 2.
[153] EUT: Digital Rights Ireland Ltd. C-293/12 ja EUT: Kärtner Landesregierung, C-594/12, kohta 71.
[154] EUT: Digital Rights Ireland Ltd. C-293/12 ja EUT: Kärtner Landesregierung, C-594/12, kohta 73.
Ks. myös Ollila 2014, s. 814, todennut samansuuntaisesti.
[155] Ks. EUT: Digital Rights Ireland Ltd. C-293/12 ja EUT: Kärtner Landesregierung, C-594/12, kohdat 15, 18, 20 ja 21.
[156] EU:n perusoikeuskirjan soveltamista koskeva kertomus vuodesta 2014, s. 13.

EU:ssa on havahduttu siihen, että henkilötietojen kerääminen, jakaminen ja käyttäminen ovat lisääntyneet. On nähty tarpeelliseksi säätää aiempaa tehokkaampaa lainsäädäntöä yksityisyyden sekä henkilötietojen suojan turvaamiseksi. Unionin tuomioistuin onkin tuonut esille, että myös kolmansissa valtioissa perustetuilla yhtiöillä, jotka ovat sijoittautuneet EU:n alueelle rekisterinpitäjinä, on velvollisuus noudattaa EU:n tietosuojalainsäädäntöä, joka tarkoittaa tietosuoja-asetuksen sekä perusoikeuskirjan 7 ja 8 artiklan huomioonottamista toiminnassaan.[157]

Unionin tuomioistuin on myös todennut tapauksessa, jossa Facebook siirtää Yhdysvaltoihin käyttäjiensä henkilötietoja sekä säilyttää niitä siellä, että eurooppaoikeuden ja erityisesti perusoikeuskirjan 8 artiklan valossa on kansallisten valvontaviranomaisten voitava tutkia itsenäisesti henkilöiden esittämiä vaatimuksia oikeuksiensa ja vapauksiensa toteuttamiseksi henkilötietojen käsittelyssä.[158] Edellä mainitut ratkaisut johtavat siihen, että rekisterinpitäjän tulee varmistua, siirtäessään henkilötietoja kolmansiin valtioihin, että henkilötietoja vastaanottava yhtiö täyttää eurooppaoikeuden mukaiset vaatimukset, joita henkilötietojen käsittelylle asetetaan. Mikäli henkilötietoja siirretään organisaation sisällä kolmansiin valtioihin, on tällöinkin luonnollisesti huolehdittava, että tietosuojaa koskevat eurooppaoikeudelliset vaatimukset edelleen täyttyvät.[159]

On huomattava, että EU:n perusoikeuskirja muodostaa ainoastaan henkilötietojen käsittelyn vähimmäistason, joka on määritelty yksityiskohtaisemmin yleisessä tietosuoja-asetuksessa.[160] Monessa kohdin kansalliselle lainsäädännölle on annettu kuitenkin liikkumavaraa, joka voi johtaa jopa yleistä tietosuoja-asetusta tiukempiin tietosuojavaatimuksiin kansallisessa lainsäädännössä. Tämän takia kansallinen lainsäädäntö tulee myös edelleen huomioida tietosuojavelvoitteita selvitettäessä.

### 3.2. Euroopan unionin tietosuojaoikeudellinen erityislainsäädäntö

Heti alkuun on syytä todeta, että asiaa sääntelevä erityislaki syrjäyttää yleislain *lex specialis derogat legi generali* -periaatteen mukaisesti. Eurooppaoikeudellisen säädöshierarkian kannalta ei ole olennaista, onko syrjäyttävä erityissäädös direktiivi, asetus vai päätös, sillä vallitsevan oikeustilan mukaan jokin edellä mainituista instrumenteista voi olla niin sanotusti sääntelyn perustava. Selvää on ainoastaan se, että unionin lainsäädännössä sekundaarilähteiden on perustuttava primaarilähteisiin ja sellaiset oikeuslähteet, jotka eivät ole Euroopan parlamentin ja neuvoston antamia, ovat edellä mainittuja instrumentteja alemman asteisia. Tällöin eurooppaoikeudellisen säädöshierarkian kannalta olennaista on se, onko kyseessä lainsäädännöllinen, delegoitu vai täytäntöönpaneva säädös. Lainsäädännöllinen säädös on sekundaarilähteiden välisessä säädöshierarkiassa korkeimmalla tasolla, ja tällainen säädös voi olla Euroopan unionin ja neuvoston asetus, direktiivi tai päätös. Kun

[157] EUT: Google Spain ja Google, C-131/12, kohta 58.
[158] EUT: Schrems, C-362/14, kohta 63.
[159] Tämän takia GDPR:n 40 artiklan mukaan kansainväliselle konsernille voidaan määritellä hyväksytyt käytännesäännöt, joita tulee noudattaa, kun henkilötietoja siirretään organisaation sisällä kolmansiin valtioihin.
[160] Ks. esim. TATTI-mietintö 35/2017, s. 58—67.

kyse on säädöshierarkian samalla tasolla olevasta instrumentista, on lex specialis -periaate sovellettavissa.[161]

*Sähköinen viestintä*

Euroopan unioni on pyrkinyt säätämään asetusta yksityiselämän kunnioittamisesta ja henkilötietojen suojasta sähköisessä viestinnässä (*sähköisen viestinnän tietosuoja-asetus*). Sen tarkoituksena olisi kumota direktiivi 2002/58/EY (*Sähköisen viestinnän tietosuojadirektiivi*). Suunniteltu asetus, kuten sillä kumottava direktiivikin ovat erityissäädöksiä (*lex specialis*) suhteessa yleiseen tietosuoja-asetukseen, jota sähköisen viestinnän tietosuoja-asetuksella olisi tarkoitus täsmentää ja täydentää henkilötiedoiksi luokiteltavien sähköisen viestinnän tietojen osalta. Vaikka sähköisen viestinnän tietosuojadirektiivi onkin erityissäädös suhteessa yleiseen tietosuoja-asetukseen, on GDPR:n säätäminen johtanut siihen, että osa direktiivin säännöksistä on kumottu, kuten sen 4 artiklan turvallisuusvelvoitteet.[162]

Globalisoituneessa verkkoyhteiskunnassa unionin sähköistä viestintää koskevalla erityissääntelyllä on hyvin keskeinen rooli tietosuojan kannalta. Sosiaalisen median ja muiden sähköisten viestintäpalveluiden merkityksen myötä suuri osa henkilötiedoista on esimerkiksi välitystietoina[163] nimenomaisesti sähköistä viestintää koskevan erityislainsäädännön kohteena.[164] Sääntelypaine sähköisen viestinnän alueella on havaittu Euroopan komission laatimassa unionin digitaalisten sisämarkkinoiden strategiassa (*DSM-strategia*) suhteellisen voimakkaaksi muun muassa digipalveluihin kohdistuvan luottamuksen kannalta. Erityisesti sähköisen viestinnän palveluiden tietoturvallisuudesta on kannettu huolta unionin kansalaisten keskuudessa.[165] Lisäksi DSM-strategiassa on todettu sähköisen viestinnän tietosuojadirektiivin jääneen osittain jälkeen vastatakseen sosiaalisen median sävyttämän verkkoyhteiskunnan kehityksen luomiin uusiin haasteisiin. Ei-toivottu markkinointiviestintä on myös osoittautunut ongelmalliseksi ilmiöksi unionin alueella. Sähköisen viestinnän tietosuoja-

[161] Craig et al. 2015, s. 106. "*Regulations are not therefore 'superior' to directives or vice versa. - - There may, for example, be a 'foundational' regulation, and directives or decisions may be made pursuant to this. The 'foundational' provision may equally be a directive or a decision.*"; Ks. myös SEUT:n 288 artikla EU:n asetuksista, direktiiveistä ja päätöksistä. Jos primaarioikeudessa ei määritellä, mitä säädöstyyppiä tulee käyttää, on sääntelykeino valittava suhteellisuusperiaatteen mukaisesti ja sääntelyalueen määrittelyssä on kunnioitettava subsidiariteettiperiaatetta. Näin ollen sääntelyn perustavassa säädöksessä on mainittava sääntelyn peruste SEUT:n 296 artiklan mukaisesti. Ks. asiaan liittyen lisäksi SEUT:n 297 artikla sekä EUT: Variola v. Amministrazione delle Finanze, C-34/73, erityisesti kohta 10, jonka osalta oikeuskäytäntö ei ole muuttunut, vaikka unionin perustamissopimuksia onkin muutettu ratkaisun antamisen jälkeen.

[162] Ehdotus sähköisen viestinnän tietosuoja-asetukseksi (2017), s. 2—3.

[163] Sähköisen viestinnän palveluita koskevan lain 3.1 §:n 40-kohdan mukaan välitystiedolla tarkoitetaan "*oikeus- tai luonnolliseen henkilöön yhdistettävissä olevaa tietoa, jota käsitellään viestin välittämiseksi sekä tietoa radioaseman tunnisteesta ja radiolähettimen käyttäjästä sekä tietoa radiolähetyksen alkamisajankohdasta, kestosta ja lähetyspaikasta".* Välitystieto voi olla henkilötieto siltä osin kuin kyse on luonnolliseen henkilöön yhdistettävissä olevasta tiedoista. Muilta osin kyse ei ole henkilötietojen suojasta.

[164] Ehdotus sähköisen viestinnän tietosuoja-asetukseksi (2017), s. 2—3.

[165] DSM-strategia, s. 47—51.

asetuksessa olisikin tarkoitus säännellä tarkentaen myös suoramarkkinoinnin puitteista, sen ollessa jo sääntelyn kohteena yleisessä tietosuoja-asetuksessa.[166]

Suomessa sähköistä viestintää sääntelee nykyisin sähköisen viestinnän palveluista annettu laki (SVL, 917/2014). Laissa säädetään viestintäverkkoja ja -palveluja koskevasta infrastruktuurista palveluiden kohtuullisen saatavuuden varmistamiseksi. Lisäksi infrastruktuurin laatu ja turvallisuus ovat keskeisessä osassa säädöksessä. Perus- ja ihmisoikeuksien näkökulmasta kyse ei ole ainoastaan yksityisyyden ja henkilötietojen suojan turvaamisesta. Kuten lain 1 §:ssä todetaan, säädöksen tarkoituksena on muun ohella perustuslain 10.2 §:ssä säädetyn viestinnän luottamuksellisuuden takaaminen. Henkilötietojen ja yksityiselämän suojasta poiketen perusoikeustasoisesta viestinnän luottamuksellisuudesta puhuttaessa on luonnollisten henkilöiden suojelun ohella kyse oikeushenkilöiden yhdenmukaisesta suojelusta.

Viestinnän luottamuksellisuudesta säädettäessä perustuslaissa ei käytetä luonnolliseen henkilöön viittaavaa ilmaisua ”*jokainen*”, vaan perusoikeus on kuvattu toteamalla ainoastaan, että ”*kirjeen, puhelun ja muun luottamuksellisen viestin salaisuus on loukkaamaton*”. Myös oikeushenkilö voi olla perusoikeuden kohteena.[167] Sähköisen viestinnän tietosuoja-asetusta koskevassa ehdotuksessa todetaankin, että sähköistä viestintää koskevassa sääntelyssä on kyse luonnollisten henkilöiden ja oikeushenkilöiden perusoikeuksien- ja vapauksien suojelusta sähköisten viestintäpalveluiden tarjoamisessa ja käytössä, mukaan lukien erityisesti oikeudet yksityiselämään ja viestinnän luottamuksellisuuden kunnioittamiseen sekä luonnollisten henkilöiden suojeluun henkilötietojen käsittelyssä.[168]

Sääntely koskee SVL:n 2 §:n mukaan niin viestinnän välittäjiä kuin lisäarvon tarjoajiakin. Tässä yhteydessä ei voida kuitenkaan kattavammin syventyä sähköistä viestintää koskevaan erityissääntelyyn tutkielman rajauksellisista syistä johtuen. Kyseisen erityissääntelyalueen huomioiminen on kuitenkin tärkeätä, sillä sääntelyllä on vaikutusta moneen rekisterinpitäjään myös osoitusvelvollisuutta täytettäessä.[169] Säädöksellä kun on jonkin asteista merkitystä lähes kaikille rekisterinpitäjille, sillä melkein jokainen työnantajan ominaisuudessa toimiva organisaatio on viestintä- tai lisäarvopalvelun tilaajana sähköisen viestinnän palveluita koskevan lain 3.1 §:n 41-kohdassa tarkoitettu

[166] Ehdotus sähköisen viestinnän tietosuoja-asetukseksi (2017), s. 21. Huomaa myös, että suoramarkkinoinnissa voi olla kyse oikeutettuun etuun perustuvasta henkilötietojen käsittelystä GDPR:n johdanto-osan 47 kappaleen perusteella. Sähköisen viestinnän tietosuoja-asetuksesta annetun ehdotuksen sivulla 22 todetaankin, että erityisesti suoramarkkinoinnin edellytyksenä olevasta suostumuksesta olisi tarkoitus säätää sähköisen viestinnän tietosuoja-asetuksessa oikeustilan selventämiseksi.

[167] Ehdotus sähköisen viestinnän tietosuoja-asetukseksi (2017), s. 23—24.

[168] Ibid. s. 24.

[169] Ks. esim. Neuvonen 2016, s. 58, Riku Neuvonen toteaa viestinnän metatietojen sijoittamisen osaksi yksityisyyden ja henkilötietojen suojaa olevan erityisen tärkeää.

yhteisötilaaja, käsitellessään viestintäverkossaan käyttäjien, yleensä työntekijöidensä, viestejä, välitystietoja tai sijaintitietoja. Kyse voi olla esimerkiksi työsähköpostia koskevan palvelun tilaamisesta ja käytöstä sekä siihen liittyvästä hallinnoimisesta.

*Matkustajatiedot*

EU on säätänyt direktiivin (EU) 681/2016 matkustajarekisteritietojen (engl. *Passenger Name Record*, PNR) käytöstä terroristirikosten ja vakavan rikollisuuden ennalta estämiseksi, paljastamiseksi ja tutkimiseksi sekä tällaisiin rikoksiin liittyviä syytetoimia varten (*matkustajarekisteridirektiivi*). Matkustajarekisteridirektiivi annettiin samana päivänä kuin yleinen tietosuoja-asetuskin. Lisäksi direktiivin soveltaminen alkoi samana päivänä GDPR:n sovellettavaksi tulemisen kanssa. Terrorismin ja muun vakavan rikollisuuden EU:n vapaalle liikkuvuudelle asettaman uhan vuoksi erityissääntely on nähty erityisen tarpeelliseksi.[170] Sääntely koskee henkilötietojen käsittelyn näkökulmasta rekisterinpitäjiä, jotka toimivat lentoliikenteen harjoittajina. Lentoliikenteen matkustajarekisteritietojen käytöstä terroririkosten ja vakavan rikollisuuden torjunnassa annetun lain (*matkustajarekisterilaki*, 657/2019) 3.1 §:n 1-kohdan mukaisesti käsitteellä tarkoitetaan lentoliikenneyritystä, jolla on voimassaoleva liikennelupa tai muu vastaava lupa, johon perustuen yhtiö on oikeutettu kuljettamaan matkustajia lentoteitse.[171]

Matkustajatietoja koskeva tietosuojaoikeudellinen erityissääntely vaikuttaa matkustajan ominaisuudessa olevien rekisteröityjen tietosuojaan. Matkustajarekisterilain 3.1 §:n 5-kohdan mukaisesti sääntelyllä vaikutetaan rekisteröityjen henkilötietojen suojaan yleisten etujen suojelemiseksi, kun käsitellään matkustajarekisteritietoja. Vaikutukset ulottuvat siis lähinnä lentoliikenteenharjoittajan kannalta lentolippuvarauksen käsittelemiseksi tarpeellisiin tietoihin. Toisin sanoen erityissääntelyn kohteena ovat rekisterinpitäjän ominaisuudessa toimivat lentoyhtiöt ja henkilötietojen kategoriat, joita erityissääntely koskee, sisältyvät lentomatkustajien matkustajatietoihin.

*Hallintotoimintaa koskeva erityissääntely*

Direktiivi (EU) 680/2016 säädettiin GDPR:n yhteydessä ja sen tarkoituksena on suojella luonnollisia henkilöitä jäsenvaltioissa toimivaltaisen viranomaisen suorittamassa henkilötietojen käsittelyssä rikosten ennalta estämistä, paljastamista, tutkimista tai rikoksiin liittyviä syytetoimia taikka rikosoikeudellisten seuraamusten täytäntöönpanoa varten sekä säännellä edellä mainittujen tietojen vapaata liikkuvuutta.[172] Tässä kohtaa on syytä huomata, että myös GDPR:ssä on rikostuomioihin ja rikkomuksiin liittyvien henkilötietojen käsittelyä koskeva erityissäännös. Direktiivin tarkoituksena on tarkentaa yleissäädöksenä toimivan tietosuoja-asetuksen sääntelyä siltä osin kuin henkilötietojen

[170] HE 55/2018 vp, s. 7—8.
[171] Ibid. s. 48—49.
[172] Direktiivin 680/2016 1(1) artikla.

käsittely kuuluu direktiivin soveltamisalaan. Käytännössä direktiivi koskee ainoastaan julkista sektoria. Toisaalta PL 124 §:n mukaan julkisia tehtäviä on mahdollista ulkoistaa yksityisille toimijoille, kunhan kyse ei ole merkittävästä julkisen vallan käytöstä. Kuitenkin GDPR:n 10 artiklassa todetaan, että ”*kattavaa rikosrekisteriä pidetään vain julkisen viranomaisen valvonnassa*”. Näin ollen sanotun toiminnan on oltava julkisen vallan tarkoin valvomaa myös silloin, kun käsittely tapahtuu yksityisoikeudellisen organisaation toimesta.

Toinen hallintotoiminnassa tapahtuvaa henkilötietojen käsittelyä koskeva erityissäädös sitoo ainoastaan Euroopan unionia sen omassa toiminnassaan. Asetuksessa (EU) 1725/2018 (*EU:n toimintaa koskeva tietosuoja-asetus*) on kyse yksilöiden suojelusta unionin toimielinten, elinten ja laitosten suorittamassa tietojenkäsittelyssä ja kyseisten henkilötietojen vapaan liikkuvuuden sääntelystä. Asetuksen päätavoitteena on yksilöiden henkilötietojen suojaa koskevan perusoikeuden suojeleminen samalla aikaansaaden puitteet tietojen vapaalle liikkuvuudelle.[173]

EU:n toimintaa koskeva tietosuoja-asetus syrjäyttää GDPR:n siltä osin, kun kyse on toiminnasta, joka asettuu sen soveltamisalaan ja näin ollen tarkentavan sääntelyn kohteeksi. EU:n toimintaa koskevan tietosuoja-asetuksen 3 artiklassa säädetyt määritelmät ovat yhdenmukaisia GDPR:n mukaisten määritelmien kanssa. Tiettyjä tarkentavia käsitteitä suhteessa GDPR:ään kuitenkin löytyy. Näistä esimerkkinä voidaan mainita *operatiivisen henkilötiedon* -käsite, jota ei erikseen määritellä yleisessä tietosuoja-asetuksessa. EU:n toimintaa koskevan tietosuoja-asetuksen 5(1)(3) artiklan mukaan sillä tarkoitetaan yleisen tietosuoja-asetuksen kanssa samansisältöisen henkilötietomäärittelmän mukaisia henkilötietoja, joita kuitenkin käsitellään SEUT:ssa säädetyn rikosoikeudellisen- tai poliisiyhteistyön puitteissa EU:n toimielinten, elinten tai laitosten toimesta.

## III. OSOITUSVELVOLLISUUS TIETOSUOJAOIKEUDELLISENA OIKEUSPERIAATTEENA

### 1. Osoitusvelvollisuuden sisältö

Osoitusvelvollisuus on määritelty yleisen tietosuoja-asetuksen 5 artiklassa, ja kansallista tietosuojalakia koskevassa hallituksen esityksessä on katsottu, ettei sen osalta tarvita erillistä lainsäädäntöä.[174] Tietosuoja-asetuksessa säädetään lisäksi tietojenkäsittelyn poikkeustilanteista. On huomattava, että osoitusvelvollisuus soveltuu myös asetuksen 85 artiklassa tarkoitettuun sananvapauteen ja tiedonvälitykseen liittyvään henkilötietojen käsittelyyn siltä osin, kun kyse on tietosuoja-asetuksen 5(1) artiklassa mainituista periaatteista.[175] Periaatteita, joiden noudattamisen *rekisterinpitäjän*

[173] EU:n toimintaa koskevan tietosuoja-asetuksen 1(1) ja 1(2) artiklat.
[174] HE 9/2018 vp, s. 50.
[175] Ibid. s. 111.

tulee kyetä aina osoittamaan toiminnassaan toteutuvan, ovat yleisen tietosuoja-asetuksen 5 artiklan 1 kohdan mukaan

- lainmukaisuus, kohtuullisuus ja läpinäkyvyys
- käyttötarkoitussidonnaisuus
- tietojen minimointi
- täsmällisyys
- säilytyksen rajoittaminen
- eheys ja luottamuksellisuus.

On syytä huomata, että vaikka eurooppaoikeus ei aikaisemmin ole edellyttänyt osoitusvelvollisuutta, on OECD vuonna 1980 julkaisemassaan ohjeessa koskien henkilötietojen suojaa ja henkilötietojen siirtämistä[176], määritellyt hyvin vastaavanlaisen periaatteen, jonka tarkoituksena oli edistää tietosuojaperiaatteiden noudattamista.[177]

### 1.1. Lainmukaisuus, kohtuullisuus ja läpinäkyvyys

Osoitusvelvollisuus edellyttää, että rekisterinpitäjän on kyettävä osoittamaan toiminnassaan noudattavansa yleisen tietosuoja-asetuksen mukaisia tietosuojaperiaatteita, jotka ilmentävät kokonaisuudessaan asetuksen tietojenkäsittelylle luomia vaatimuksia. GDPR:n 5(1)(a) artiklan mukaan henkilötietoja ”*on käsiteltävä lainmukaisesti, asianmukaisesti ja rekisteröidyn kannalta läpinäkyvästi (’lainmukaisuus, kohtuullisuus ja läpinäkyvyys’)”*. Näin ollen läpinäkyvyyden periaatteen osalta, kyse ei ole niinkään ensisijaisesti yleisöjulkisuudesta tai siitä, että toiminta olisi riittävän läpinäkyvää suhteessa viranomaiseen. Läpinäkyvyyden vaatimusta on arvioitava nimenomaisesti rekisteröityyn nähden. Osoitusvelvollisuus oikeusperiaatteena puolestaan luo puitteet tietosuojaviranomaiselle suuntautuvalle läpinäkyvyydelle.

Läpinäkyvyys on ainoa yleisen tietosuoja-asetuksen 5(1)(a) artiklan sisältämistä periaatteista, jonka tulkinnassa ei voida hyödyntää GDPR:n sovellettavaksi tulemista edeltänyttä oikeuskäytäntöä, sillä sitä ei mainita itsenäisenä tietosuojaperiaatteena henkilötietodirektiivissä.[178] Läpinäkyvyyden laadulle asetetaan lisävaatimukseksi tietosuoja-asetuksen 12(1) artiklassa se, että rekisteröidylle annettavan käsittelyä koskevan informaation on oltava *”helposti ymmärrettävässä ja saatavilla ole-*

[176] Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of the Personal Data, 23.9.1980, kohta 14, *Accountability Principle*: “*A data controller should be accountable for complying with measures which give effect to the principles stated above.”* On syytä huomata, että myös GDPR:n mukainen osoitusvelvollisuus on englanniksi *accountability*. Lisäksi myös GDPR:n mukaisessa osoitusvelvollisuudessa, periaate koskee nimenomaisesti rekisterinpitäjää ja kyse on siitä, että rekisterinpitäjän tulee kyetä osoittamaan noudattavansa muita tietosuojaperiaatteita erinäisin toimenpitein.
[177] Kremer 2016, s. 133.
[178] Ks. henkilötietodirektiivin 6(1)(a) artikla.

*vassa muodossa selkeällä ja yksinkertaisella kielellä"*. Koska läpinäkyvyyttä on arvioitava rekisteröidyn näkökulmasta ja käsittelyprosessit saattavat olla joskus hyvinkin monimutkaisia, mahdollistaa GDPR:n 12(1) artikla tietyn asteisen harkintavallan käyttämisen sen suhteen kuinka yksityiskohtaisia tietoja rekisteröidyille ensiasteessa annetaan[179]. Olennaista on se, että rekisteröity saa kaiken näkökulmastaan tarpeellisen tiedon ymmärrettävässä muodossa[180]. Ennen kaikkea kyse on rekisteröidyn ja rekisterinpitäjän välille muodostuvan luottamussuhteen ylläpitämisen puitteet informaation avulla aikaansaatavista fasiliteeteista.[181]

GDPR:n 5(1)(a) artiklan rakenteesta päätellen asianmukaisuudella viitataan kohtuullisuuden periaatteeseen. Käsittely on asianmukaista ainoastaan silloin, kun sillä ei kohtuuttomasti puututa rekisteröidyn henkilötietojen suojaan. Lisäksi käsittelyperusteiden ja -tarkoitusten asianmukaisuutta arvioitaessa huomio on kiinnitettävä siihen, että käsittely olisi rekisteröidyn näkökulmasta kohtuudella hyväksyttävää. On huomattava, että englanninkielessä ilmaisu "*fairness*", on jokseenkin monimerkityksisempi kuin suomenkielessä käytetty ilmaisu "*kohtuullisuus*". Näin ollen on perusteltua ymmärtää kohtuullisuus laajemmin yleisen tietosuoja-asetuksen mukaista kohtuullisuutta tulkittaessa. Tällöin kohtuullisuuteen voidaan liittää myös oikeudenmukaisuuden ja reiluuden ajatukset. Varmasti myös tämän takia GDPR:ssä kohtuullisuus on linkitetty kiinteästi yhteen lainmukaisuuden kanssa. Englanninkielistä ilmaisua "fairness" voidaankin pitää suomenkielisessä versiossa käytettyä käsitettä kuvaavampana ainakin tietosuoja-asetuksen kontekstissa.[182]

[179] On huomattava, että annettavien tietojen vaadittavan yksityiskohtaisuuden asteen arvioimisessa informaation yksinkertaisuuteen ja selkeyteen vetoamalla ei voida jättää mitään rekisteröidyn kannalta olennaista ilmoittamatta. Toisaalta informointivelvollisuutta ei täytetä kokonaisuudessaan organisaation monesti kaikki käsittelytoimet kattavalla informoinnilla (*Privacy Notice*). Onkin järkevää, että rekisterinpitäjä laatii tiettyjä käsittelyprosesseja koskevia dokumentteja, joita voidaan hyödyntää rekisteröidyn halutessa lisätietoja. Annettavan tiedon määrään vaikuttaa myös tietoturvallisuuden periaate, jonka toteutumista informoinnin ei tule vaarantaa. Ks. lisäksi Article 29 Data Protection Working Party, WP 260, läpinäkyvyyden toteuttamisesta käytännössä.

[180] Esim. rekisteröidyn antaessa suostumuksen potilastietojensa näkyvyydelle myös yksityisten terveydenhuoltopalveluiden tuottajille, ei ole olennaista, että tällaisessa tilanteessa luetellaan kaikki Suomen yksityiset terveydenhuoltopalveluiden tarjoajat, vaikka rekisteröidyllä on sinänsä oikeus tietää, kenellä kaikilla kolmansilla osapuolilla on pääsy tämän henkilötietoihin. Rekisteröity saa riittävän kuvan paljon selkeämmässä muodossa, mikäli suostumuksen todetaan koskevan ainoastaan yksityisten terveydenhuoltopalveluiden tuottajien tiedonsaantioikeuksia.

[181] Article 29 Data Protection Working Party, WP 260, s. 6.

[182] Ks. Koskinen 2018, s. 243—244, kohtuullisuuden suomen yleiskielistä määritelmää laajemmasta merkityksestä tietosuoja-asetuksen kontekstissa.

Myös suomalaisessa oikeustieteessä on eksplisiittistä tulkintakäytäntöä laajasti sitä, mitä kohtuullisuudella tarkoitetaan. Tällöin kohtuullisuuden on nähty olevan yhteydessä suhteellisuuden periaatteeseen ainakin hallinto-oikeudellisessa tutkimuksessa ja oikeuskäytännössä.[183] Eurooppaoikeudellisesta *yhtenäisen tulkinnan vaatimuksesta*[184] johtuen, pitäydyn kuitenkin arvioimaan kohtuullisuuden periaatetta nimenomaisesti ”fairness” -tulkintalinjasta käsin. Tämä johtuu siitä, että GDPR:n lainsäädäntöprosessi suoritettiin englanniksi ja lisäksi EU:n yleisen tietosuoja-asetuksen yhtenäistä tulkintaa ylläpitävät elimet antavat ohjeensa englanninkielellä.[185] Laajemmin tarkasteltuna kohtuullisuuden periaate on myös eurooppalaisen hallinto-oikeuden keskeinen hyvän hallinnon periaatteen elementti. On kuitenkin huomattava, että Euroopan hyvän hallintotavan säännöstön 11 artiklassa mainittu ”*fairness*” on käännetty säädöksen suomenkielisessä versiossa oikeudenmukaisuudeksi.[186]

Koska kohtuullisuus on rakenteellisesti yhdistettävissä asianmukaisuuteen tietosuoja-asetuksen kielenkäytössä ja rakenteessa, on luontevaa huomioida kohtuullisuuden tulkinnassa se, mitä todetaan asianmukaisuudesta yleisen tietosuoja-asetuksen johdanto-osassa. Esimerkiksi asetuksen automatisoitua päätöksentekoa koskevaa 22 artiklaa täsmentävän asetuksen johdanto-osan 71 kappaleen mukaan rekisteröityä koskevan asianmukaisen ja läpinäkyvän käsittelyn varmistamiseksi rekisterinpitäjän tulee suojata henkilötiedot siten, että estetään muun muassa luonnollisten henkilöiden syrjintä rodun tai etnisen alkuperän taikka muun niihin rinnastettavissa olevan syyn perusteella. Voidaankin huomata, että käsittelyn asianmukaisuus ja kohtuullisuus tarkoittavat ennen muuta sitä, että käsittelyssä kunnioitetaan tietosuojan lisäksi myös muita rekisteröidyn perus- ja ihmisoikeuksia, kuten oikeutta yhdenvertaisuuteen.[187]

Käsittelyn lainmukaisuudella on ymmärrettävä tarkoitettavan ennen kaikkea sitä, että käsittelylle on jokin GDPR:n 6 artiklassa määritelty oikeusperuste[188] sen ohella, että käsittelyprosessissa omaksutut tekniset ja organisatoriset toimenpiteet ovat riittäviä tietosuoja-asetuksen 5 artiklan mukaisten

---

[183] Ks. esim. KHO 2011:664 ja Korte 2015, s. 8, joissa ilmenee kohtuullisuuden ja suhteellisuuden periaatteiden välinen suhde hallinto-oikeuden oikeudenalalla.

[184] Craig et al. 2015, s. 186, 197, 209, 366 ja 369, yhtenäisen tulkinnan vaatimus pätee erityisesti suoran vaikutuksen omaavissa suoraan sovellettavissa instrumenteissa kuten asetuksissa. Näin ollen yhtenäisen tulkinnan vaatimusta tulee noudattaa myös yleisen tietosuoja-asetuksen osalta. Vastaavan suuntaisesti on todettu jopa direktiiveistä (EUT: Association de médiation sociale (AMS) v. Union Locale des syndicats CGT, Laboudi and others, C-176/12, kohdat 49, 50 ja 51); Ks. myös esim. Raitio 2013, s. 251, eurooppaoikeuden ensisijaisuudesta ja SEU 4(3) artikla lojaliteettiperiaatteesta ja velvoitteesta edistää integraatiota.

[185] Näitä elimiä ovat EU:n tietosuojatyöryhmä (Article 29 Data Protection Working Party) sekä Euroopan tietosuojaneuvosto (EDPB, European Data Protection Board).

[186] Euroopan hyvän hallintotavan säännöstön 11 artikla *Oikeidenmukaisuus* (engl. *Fairness*): ”*Virkamiehen on toimittava puolueettomasti, oikeudenmukaisesti ja kohtuullisesti*”. Englanninkielisessä versiossa säännöksen jälkimmäinen maininta kohtuullisuudesta on ilmaistu sanalla ”*reasonably*” ja ilmaisussa ”*oikeudenmukaisesti*” on käytetty ”*Fairly*” -sanaa.

[187] Tzanou 2013, s. 89.

[188] Huomaa myös, että GDPR:n johdanto-osan 40 kappaleessa todetaan henkilötietojen käsittelyn lainmukaisuuden edellyttävän, että käsittely perustuu rekisteröidyn suostumukseen taikka muuhun GDPR:n 6 artiklassa mainittuun oikeutettuun käsittelyperusteeseen. Henkilötietojen erityisryhmiin kuuluvia tietoja käsiteltäessä on puolestaan huomioitava se, mitä näiden tietojen käsittelystä säädetään GDPR:n 9 artiklassa.

tietosuojaperiaatteiden toteuttamisen takaamiseksi.[189] Edellä mainitun lisäksi henkilötietojen käsittelyssä on noudatettava myös muutakin lainsäädäntöä kuin tietosuojaoikeudellisia säädöksiä. Tästä hyvänä esimerkkinä voidaan mainita perusoikeuksien noudattaminen, jota voidaan nähdä jo edellä esitetyn kohtuullisuudenkin edellyttävän.[190] Tutkielman III osan jälkivalvontaa koskevassa 4.5. luvussa otetaan kantaa siihen, missä määrin tietosuojaviranomainen voi toimivaltansa puitteissa valvoa muun kuin tietosuojalainsäädännön noudattamista sekä voiko tällaisen lainsäädännön noudattamatta jättäminen johtaa GDPR:n mukaisten hallinnollisten sakkojen määräämiseen.

### 1.2. Käyttötarkoitussidonnaisuus

Yleisen tietosuoja-asetuksen 5(1)(b) artiklan mukaan henkilötiedot on *"kerättävä tiettyä, nimenomaista ja laillista tarkoitusta varten, eikä niitä saa käsitellä myöhemmin näiden tarkoitusten kanssa yhteensopimattomalla tavalla; myöhempää käsittelyä yleisen edun mukaisia arkistointitarkoituksia taikka tieteellisiä ja historiallisia tutkimustarkoituksia tai tilastollisia tarkoituksia varten ei katsota 89 artiklan 1 kohdan mukaisesti yhteensopimattomaksi alkuperäisen tarkoituksen kanssa"*. Kuten säännöksen sanamuodosta ilmenee, käyttötarkoitussidonnaisuudella on läheinen yhteys lainmukaisuuden vaatimuksen kanssa. Kun käsittelylle on ensin määritetty lainmukainen käyttötarkoitus, on jatkossa huolehdittava, ettei kyseisiä henkilötietoja käsitellä myöhemmin muita käyttötarkoituksia varten, ellei myöhempi käsittely tapahdu yleisen edun mukaisia arkistointitarkoituksia tai tieteellisiä, historiallisia taikka tilastollisia käsittelytarkoituksia varten.

Käyttötarkoitussidonnaisuus on jo henkilötietodirektiivin aikakaudelta tuttu tietosuojaperiaate. Näin ollen sen tulkinnassa on perusteltua hyödyntää myös henkilötietolain esitöitä sekä ennen tietosuoja-asetuksen sovellettavaksi tulemista syntynyttä oikeuskäytäntöä ja -kirjallisuutta. Henkilötietojen käsitteleminen tapahtuu aina jotakin tiettyä käyttötarkoitusta varten ja myös henkilörekisterit on luotu tiettyjen tehtävien suorittamiseksi, muutoinhan käsittely ei edes voisi olla rationaalista. Toisaalta käsittelyn logiikka ei välttämättä kokonaisuudessaan ilmene yhdestä henkilörekisteristä käsin, vaan samoissa käsittelyprosesseissa saatetaan hyödyntää useammassa eri henkilörekisterissä olevia henkilötietoja. Näin ollen käyttötarkoitusten arvioiminen on enemmän prosessikohtaista kuin henkilörekisterikohtaista.[191] Henkilörekisterin spesifikaateissa voidaan ja tuleekin määritellä, mihin tarkoituksiin rekisterissä olevia tietoja käsitellään jo tietoturvallisuuden periaatteesta johtuen, kun oikeudeton tietojen paljastuminen ja tietoihin pääsy tulee estää luottamuksellisuuden varmistamiseksi.

Henkilötietojen käsittelyn käyttötarkoitussidonnaisuuden ydinsisältönä on se, että tietojenkäsittelylle ennen sen aloittamista määritelty käyttötarkoitus rajaa sitä, mihin tarkoituksiin henkilötietoja

[189] De Hert et al. 2016, s. 187.
[190] Article 29 Data Protection Working Party, WP 203, s. 9—11 ja 14—15.
[191] Tietosuojavaltuutetun toimiston ohje (2010), s. 6.

on sallittua hyödyntää. Tämä johtaa siihen, ettei tiettyä tarkoitusta varten kerättyjä henkilötietoja saa myöhemmin yhdistää toiseen käyttötarkoitukseen perustuvaan käsittelyprosessiin niin, että nämä tiedot tulisivat myöhemmin hyödynnetyksi yhdessä muiden henkilötietojen kanssa jotakin eri käyttötarkoitusta varten.[192] Käyttötarkoitussidonnaisuus sitoo sekä rekisterinpitäjää että henkilötietojen käsittelijöitä, minkä takia GDPR:n 28(10) artiklassa todetaan, että henkilötietojen käsittelijää, joka rikkoo käsittelylle asetettua tarkoitusta ja keinoa, on pidettävä rekisterinpitäjänä sanotun käsittelyn osalta. Tämä myös ilmentää sitä, että nimenomaan rekisterinpitäjän tehtävänä on määritellä henkilötietojen käsittelyn käyttötarkoitus, jota henkilötietojen käsittelijöidenkin on noudatettava käyttötarkoitussidonnaisuuden periaatteen nojalla.

Arvioitaessa poikkeamisperusteita käyttötarkoitussidonnaisuudesta, voidaan kiinnittää huomiota hallituksen esitykseen, jonka mukaan tieteellinen ja historiallinen tutkimus tulee ymmärtää samalla tavoin kuin se yleensä ymmärretään.[193] Näin ollen tulisi käyttää sanamuodon yleiskielen mukaista tulkintaan. Korkein hallinto-oikeus on ratkaisussaan KHO 2013:181 todennut, että tieteelliseltä tutkimukselta edellytetään esimerkiksi autonomisuutta ja julkisuutta. Tutkimuksen ei siis tule tapahtua pelkästään tietyn organisaation taloudellisista näkökohdista käsin. Lisäksi tutkimuksen suorittavalla henkilöllä tulee olla riittävä pätevyys tieteelliseen tutkimukseen. Kyse ei näin ollen voi olla pelkästä keinotekoisesta järjestelystä, jonka avulla käyttötarkoitussidonnaisuudesta voitaisiin poiketa. Tietosuojavaltuutettu onkin ratkaisussaan TSV 17.5.2017[194] todennut, että kun tutkimustulosten raportoinnissa ei ole yksilöity, miten ne saatetaan julkisesti tiedeyhteisön arvioitaviksi ja kun tutkimuksen yhteenvetoraportti suunnataan pelkästään tutkimuksen rahoittajalle, asettuu tutkimuksen autonomisuus kyseenalaiseksi. Näin ollen henkilötietoja ei voitu myöhemmin käsitellä alkuperäiseen käyttötarkoitukseen nähden poikkeaviin tarkoituksiin tieteellistä tutkimusta koskevan poikkeussäännöksen nojalla.

Toinen käyttötarkoitussidonnaisuutta koskeva poikkeus soveltuu yleisen edun mukaisiin arkistointitarkoituksiin.[195] GDPR:n johdanto-osan 156 kappaleen mukaan yleisen edun mukaisten arkistointitarkoitusten käsillä ollessakin tulisi noudattaa asetuksen rekisteröidyn oikeuksia ja vapauksia koskevia asianmukaisia suojatoimia. Tietosuojalakia koskevan hallituksen esityksen mukaan julkishallinnolla tai yksityisellä sektorilla voi olla hallussaan yleistä etua koskevia tietokantoja ja niiden avulla suoritettuja palveluita, joilla on pysyvää yleistä etua koskeva merkitys. GDPR:n johdanto-

[192] Sorvari et al. 2006, s. 128.
[193] HE 96/1998 vp, s. 17 ja 45.
[194] On huomattava, että kannanotto annettiin aikana, jolloin GDPR oli voimassa, mutta sitä ei vielä sovellettu, joten tarkoituksena oli ennen kaikkea linjata myöhemmin sovellettavaksi tulevan tietosuoja-asetuksen tulkintaa, eikä kyseessä näin ollen ollut vielä GDPR:n mukainen tietosuojaviranomaisen päätös.
[195] Etenkin yleisen edun mukaisten arkistointitarkoituksien sekä historiallisten tarkoituksien osalta huomionarvoista on se, että GDPR:n johdanto-osan 27 ja 158 kappaleen mukaisesti yleinen tietosuoja-asetus ei sovellu kuolleiden henkilöiden henkilötietoihin. Tällöin GDPR:n mukaisia tietosuojaperiaatteita ei tarvitse noudattaa.

osan 158 kappaleessa todetaankin, että jäsenvaltiolla on mahdollisuus säätää tällaisesta arkistotoiminnasta kansallisella lailla. Lisäedellytyksenä tietosuoja-asetuksen 89(1) artiklassa todetaan, että käsittelyn on oltava oikeassa suhteessa sen tavoitteisiin nähden sekä asetuksen takaamaa oikeutta henkilötietojen suojaan on poikkeussäännöksestäkin huolimatta pyrittävä toteuttamaan keskeisiltä osin. Toisaalta myös perustuslain nojalla edes tavallisella lailla ei voida puuttua yksilön yksityisyyden tai henkilötietojen suojan ydinalueeseen.[196]

### 1.3. Tietojen minimointi

Yleisen tietosuoja-asetuksen 5(1)(c) artiklan mukaan *"henkilötietojen on oltava asianmukaisia ja olennaisia ja rajoitettuja siihen, mikä on tarpeellista suhteessa niihin tarkoituksiin, joita varten niitä käsitellään"*. Säännöksestä ilmenee tietojen minimointiperiaatteen yhteys edellä kuvattuun käyttötarkoitussidonnaisuuteen. Käsittelyn tarpeellista laajuutta on arvioitava nimenomaan käsittelylle määritellystä tarkoituksesta käsin. Toisaalta henkilötietojen suoja joutuu joissain tilanteissa konfliktiin suhteessa muihin perusoikeuksiin. Esimerkiksi sananvapaudesta johtuen on todettu, että tietojen minimointiperiaatteen soveltaminen ei ole tarkoituksenmukaista, kun henkilötietojen käsittely perustuu journalistisiin tarkoituksiin tai kun kyse on taiteellisesta, akateemisesta taikka kirjallisesta ilmaisusta.[197] Edellä kuvattuihin tarkoituksiin tarvitaan monesti poikkeuksellisen laajoja tietovarantoja käsittelylle määritellyn tarkoituksen toteuttamiseksi. Tällöin lähtökohtana ei voida pitää tietojen minimointiperiaatteen mukaista näkökulmaa. Toisaalta tämäkään ei mahdollista poikkeamista muista tietosuojaperiaatteista.[198]

Apulaistietosuojavaltuutettu on todennut rekisteröidyn tunnistamista ja puheluiden tallentamista koskevassa ratkaisussaan TVS 22.11.2019[199], että tarpeettomien tietojen pyytäminen rekisteröidyltä tämän tunnistamiseksi on tietojen minimointiperiaatteen vastaista. Tapauksessa rekisterinpitäjä oli pyytänyt rekisteröidyltä tämän tunnistamiseksi lisätietoina muun muassa henkilötodistuksen tai kopion passista sekä valokuvan kyseisen todistuksen kanssa. Tässäkin tapauksessa on merkille pantavaa, että tietojen minimointia arvioitiin nimenomaan henkilötietojen käyttötarkoituksen näkökulmasta. Huomiota kiinnitettiin myös kyseisten tietojen funktioon ja tunnistautumista koskeviin erityissäännöksiin. Näin ollen tietojen minimointiperiaatteen perusteella rekisterinpitäjän on oikeus käsitellä vain sellaisia henkilötietoja, jotka ovat käyttötarkoitussidonnaisuuden nojalla välittömästi

---

[196] HE 9/2018 vp, s. 25.

[197] HE 9/2018 vp, s. 57—61: Tietosuojalaissa päätettiinkin käyttää kansallista liikkumavaraa siten, että sananvapauden suojaamisen nojalla myös journalistisiin ja taiteellista sekä kirjallista ilmaisua koskeviin tarkoituksiin käytettävään henkilörekisteriin ei sovelleta tietojen minimointiperiaatetta. Ks. myös tietosuojalain (1050/2018) 27 §, kyseisen liikkumavaran käytöstä. Näin ollen käyttötarkoitus määrittää poikkeuksen sovellettavuuden ja käyttötarkoitussidonnaisuus sen laajuuden.

[198] Ks. myös vireillä oleva HE 2/2020 vp, jonka johdosta saattaa tulla uusia poikkeuksia oikeusministeriön hallinnonalaa koskevaan erityislainsäädäntöön erityisesti tilastollisia tarkoituksia ajatellen.

[199] Ratkaisu sisältää myös toimenpidemääräyksen olla säilyttämättä käsillä olevalla tavalla hankittuja henkilötietoja.

tarpeellisia, ellei jostain muusta perusoikeudesta johtuen ole säädetty erityislainsäädäntöä tai erityissäännöksiä, joiden nojalla voidaan päätyä tästä poikkeavaan lopputulokseen.

### 1.4. Täsmällisyys

Yleisen tietosuoja-asetuksen 5(1)(d) artiklan mukaan *"henkilötietojen on oltava täsmällisiä ja tarvittaessa päivitettyjä; on toteutettava kaikki mahdolliset kohtuulliset toimenpiteet sen varmistamiseksi, että käsittelyn tarkoituksiin nähden epätarkat ja virheelliset henkilötiedot poistetaan tai oikaistaan viipymättä"*. Täsmällisyyden periaate siis jakautuu kahteen elementtiin. Ensinnäkin on huolehdittava, että henkilörekisterissä olevat henkilötiedot ovat alusta alkaen täsmällisiä. Toiseksi, on ylläpidettävä mekanismeja, joiden avulla henkilötiedot pysyvät täsmällisinä ja tarvittaessa päivittyvät myös silloin, kun kyseiset henkilötiedot eivät ole aktiivisen käsittelyn kohteena. Toisin sanoen ei voida jättää pelkästään rekisteröityjen tietojen oikaisemista koskevan oikeuden varaan sitä, että henkilötiedot pysyvät täsmällisinä ja tarkkoina.

Rekisterinpitäjän on tarpeellisin teknisin ja organisatorisin toimenpitein pyrittävä täyttämään täsmällisyysvaatimus. Rekisterinpitäjältä ei siis edellytetä mitä tahansa toimenpiteitä henkilötietojen täsmällisyyden varmistamiseksi, vaan kyse on kaikista mahdollisista kohtuullisista toimenpiteistä sanamuodon mukaisesti.[200] Käytännössä täsmällisyysvaatimus tarkoittaa siis sitä, että rekisterinpitäjä tai henkilötietojen käsittelijä

- ottaa tarkoituksenmukaiset askeleet varmistaakseen kaikkien henkilötietojen täsmällisyyden
- varmistaa, että henkilötietojen lähde ja status on selvä
- harkitsee huolella kaikkien henkilötietojen tarkkuuteen liittyviä haasteita
- harkitsee tämän pohjalta, onko henkilötietoja tarpeen päivittää säännöllisesti.

Koska henkilötietojen täsmällisyyden varmistamiseksi voidaan käyttää rajaton määrä resursseja, korostuu täsmällisyysvaatimuksen tulkinnassa GDPR:ssä omaksuttu *riskilähtöinen lähestymistapa*. Sitä, mitkä toimenpiteet lopulta nähdään kohtuullisiksi, on arvioitava siis erityisesti henkilötietojen täsmällisyyteen kohdistuvan riskin ja niiden mahdollisten seurausten näkökulmasta. Näin ollen tarpeelliset toimenpiteet hahmottuvat edellä olevan listan kolmannesta osasta eli henkilötietojen tarkkuuteen liittyvistä haasteista käsin.[201]

---

[200] GDPR:n johdanto-osan 39 kappale; ks. myös HE 2/2020 vp, s. 26, jossa todetaan saman suuntaisesti.

[201] Information Commissioner's Office (ICO eli Iso-Britannian tietosuojaviranomaisen), ohje: Principle (d): Accuracy; Huomaa myös, että ICO:n ohjeistamien esimerkkitapausten pohjalta on havaittavissa henkilörekisterissä olevien henkilötietojen käyttötarkoituksella ja käsittelyn tavoitteella olevan suuri merkitys arvioitaessa tarpeellisia ja kohtuullisia toimenpiteitä täsmällisyysvaatimuksen täyttämiseksi. Esimerkiksi postipakettien toimitusosoitteista koostuvan henkilörekisterin tavoitteena voi olla mahdollistaa yksilön vastaanottaa postipakettinsa myös eri osoitteeseen kuin missä tämä vakituisesti asuu. Näin ollen rekisterin säännöllinen päivittäminen vakituisen asuinpaikan osoitteen ja siihen liittyvien osoitteenmuutosten perusteella voisi johtaa epätoivottuun lopputulokseen.

### 1.5. Säilytyksen rajoittaminen

Yleisen tietosuoja-asetuksen 5(1)(e) artiklan mukaan henkilötietoja *"on säilytettävä muodossa[202], josta rekisteröity on tunnistettavissa ainoastaan niin kauan kuin on tarpeen tietojen käsittelyn tarkoitusten toteuttamista varten; henkilötietoja voidaan säilyttää pidempiä aikoja, jos henkilötietoja käsitellään ainoastaan yleisen edun mukaisia arkistoimistarkoituksia taikka tieteellisiä tai historiallisia tutkimustarkoituksia tai tilastollisia tarkoituksia varten --, edellyttäen, että -- asianmukaiset tekniset ja organisatoriset toimenpiteet on pantu täytäntöön rekisteröidyn oikeuksien ja vapauksien turvaamiseksi"*. Näin ollen säilytysaikojen rajoittamisen periaatetta on noudatettava, ellei käsittelyprosessiin sovellu tietosuoja-asetuksen 89 artikla, jolloin myös edellä kuvatusta käyttötarkoitussidonnaisuuden periaatteesta voidaan joustaa. Lisäksi säännöksen nojalla on todettavissa, että säilytysaikojen määrittäminen on kiinteässä yhteydessä käsittelyn käyttötarkoitukseen. Tämän takia on luontevaa, että tietosuoja-asetuksen 89 artiklan määrittämissä poikkeustilanteissa mahdollistetaan poikkeaminen käyttötarkoitussidonnaisuusperiaatteen lisäksi säilytysaikojen rajoittamisen periaatteesta. Tietosuoja-asetuksen 4(2) artiklan mukaan luonnollisesti myös tietojen säilyttäminen on henkilötietojen käsittelyä, on kyse sitten kuinka passiivisesta tietojen varastoimisesta tahansa.

Koska säilytysaikojen rajoittaminen on kiinteässä yhteydessä henkilötietojen käyttötarkoitukseen, periaatetta on luontevaa lähestyä ajatusmallista, jonka mukaan informaatio on hyödyke, jolle on mahdollista määritellä erinäisiin hyödyntämiskeinoihin liittyvin perustein arvo.[203] Informaatiolle voidaan määritellä sekä primaariarvo että sekundaariarvo. Primaariarvolla muodostetaan asiakirjan laatijalle tiedon synnyttämä käyttötarkoituksen mukainen arvo, kun taas sekundaariarvo määrittää tiedon tutkimusarvoa, joka puolestaan on jaettavissa edelleen informaatioarvoon ja todistusarvoon.[204] Tässä suhteessa säilytyksen rajoittamista on tarkasteltava tiedon primaariarvosta[205] käsin.

Tiedon käyttöarvo, johon perustuu yleensä myös tiedon taloudellinen arvo, luo siis pohjan säilytyksen rajoittamisen periaatteelle. Käyttöarvoon vaikuttaa olennaisesti tiedon hyödyntäjä sekä käyttötilanne.[206] Käyttötilanteita, sekä lähtökohtaisesi myös tiedon hyödyntäjien joukkoa, on rajoitettava tietoturvallisuuden ja käyttötarkoitussidonnaisuuden periaatteen nojalla. Tällöin käyttöarvoa on arvioitava tiettyjen ennalta määriteltyjen käyttötilanteiden valossa. Kyse on siis henkilötietojen käyttötarkoitukseen sidotusta harkinnasta. Koska säilytysaikoja on rajoitettava tiedon primaariarvosta

---

[202] Valitun sanamuodon mukaisesti tietojen anonymisoiminen sallitaan tuhoamisen ohella yhtenä keinona noudattaa tietojen säilytyksen rajoittamisen periaatetta. Kun tiedot ovat anonymisoituja, ne eivät ole enää henkilötietoja, eikä tietosuoja-asetusta näin ollen enää sovelleta kyseisten tietojen osalta, edellyttäen, että rekisteröity ei ole enää välillisesti tai välittömästi tunnistettavissa tiedoista.

[203] Voutilainen et al. 2015, s. 70—72, tiedon arvon määrittämisestä.

[204] Ks. asiakirjahallinnan arvonmääritysteorioista laajemmin Schellenberg 2003, ja erityisesti tutkielmani kontekstissa s. 14 ja 139. Teos on alun perin vuodelta 1956, mutta H.G. Jones on päivittänyt sen vuonna 2003 tälle vuosituhannelle. Teoksen keskeinen sisältö ei kuitenkaan muuttunut.

[205] Etenkin käsittelyn oikeusperusteen ollessa oikeutettu etu, on primaariarvo olennainen.

[206] Repo 1984, s. 52.

käsin, ei säilytystä voida perustella tiedolle tulevaisuudessa muodostuvien toiminnallisuuksien avulla. Toisin sanoen historiallinen ja tilastollinen sekundaariarvo saattaa muodostua vasta pitkän ajan kuluessa esimerkiksi tietovarantojen kasvaessa. Tällaiset perustelut tietojen säilyttämiselle eivät ole kuitenkaan hyväksyttäviä, mikä ilmenee suoraan säilytyksen rajoittamisperiaatetta koskevan säännöksen loppuosassa mainitusta poikkeuksesta. Sen mukaan muun muassa historiallisia ja tilastollisia tarkoituksia varten tapahtuva tietojenkäsittely on nimenomaisesti vapautettu kyseisen periaatteen noudattamisesta käsittelyn luonteen vuoksi.

Mikäli henkilötietojen käsittely perustuu puhtaasti GDPR:n 6(1)(c) artiklan mukaisen lakisääteisen velvoitteen noudattamiseen, on säilytysajan määrittäminen yleensä yksinkertaisinta, sillä monesti tällöin kyse on laissa määritellyn säilytysajan noudattamisesta, esimerkiksi valvontaviranomaisten suorittamien tarkastusten varalta. Kyse ei välttämättä kuitenkaan ole näissä tapauksissa tiedon primaariarvosta, vaan sekundaariarvolle tyypillisemmästä tiedon todistusarvosta, jotta viranomaiselle kyetään jälkikäteen osoittamaan, että lainsäädäntöä on noudatettu. Näin on asianlaita kirjanpitolain mukaisia kirjanpitoaineiston säilytysaikoja noudatettaessa, jolloin yhtiölle muodostuva tiedon primaariarvo on todellisuudessa hävinnyt jo kauan ennen laissa säädetyn säilytysajan päättymistä. Kymmenen vuotta vanhat tiedot kun eivät ole kovinkaan olennaisia yhtiön nykytilaa ja tulevaisuutta koskevassa päätöksenteossa. Tiedot kuitenkin on säilytettävä verotarkastuksien varalta. Näin ollen lakisääteisen velvoitteen täyttämiseksi suoritetun käsittelyn pohjana olevien henkilötietojen säilytysaikojen määrittelyssä tiedon primaariarvo ei poikkeuksellisesti ole määrittävä tekijä, vaan laista johtuva säilytysaika.[207]

On huomattava, että lakisääteisen velvoitteen täyttämiseksi tapahtuvan käsittelyn osalta lainsäädännössä tulisi olla myös säännökset näissä tilanteissa säilytettävien henkilötietojen säilytysajoista. Tämä johtuu siitä, että perustuslain 10.1 §:n mukaan henkilötietojen suojasta on säädettävä tarkemmin lailla. Perustuslakivaliokunta on puolestaan todennut, että kyseinen lailla säätämisen vaatimus pitää sääntelykohteiltaan sisällään käsittelyn tavoitteen, henkilötietojen sisällön, niiden sallitut

[207] Huomaa, että rekisterinpitäjän lakisääteinen velvollisuus ei ole aina yhtä selkeä säilytysajan määrittämisen kannalta. Esimerkiksi työsopimuslain (TSL, 55/2001) 6:7:n mukaan työnantajan on säilytettävä työtodistusta vähintään kymmenen vuotta työsuhteen päättymisen jälkeen. Kuitenkin työnantajan on annettava TSL:n 6:7.3:n mukaan työsuhteen päättymisestä kuluneen kymmenen vuoden jälkeenkin, lähteneelle työntekijälle, tiedot työsuhteen kestosta ja työtehtävien laadusta, jos siitä ei aiheudu kohtuutonta hankaluutta. Itseasiassa työtodistuksen säilyttämiselle työnantajan toimesta ei taida missään vaiheessa olla muu kuin työntekijän oikeuksia suojaava funktio. Tuskin on tarkoituksenmukaista, että samaisten yksilöiden suojaamiseksi säädetyn säilytyksen rajoittamisen periaatteen nojalla kaikki työtodistukset tuhottaisiin tietosuojalainsäädännön nojalla, heikentäen näin yksilön muiden intressien suojaa. Tämä olisi nimenomaan yksilön työntekijänä omaamien oikeuksien kannalta ongelmallista. Asianmukaisinta lienee olevan erityissäännöksen hengen mukaisesti hävittää selvästi työsuhteen keston ja laadun kannalta tarpeeton aines työtodistuksista tuon kymmenen vuoden määräajan kuluessa umpeen. Toisaalta voidaan kysyä, onko muunlaisen tiedon sisällyttäminen työtodistukseen koskaan asianmukaista. Lopuksi voidaan todeta, että TSL:n 6 §:ää lienee perusteltua soveltaa sen ajatellen olevan erityissäännös (lex specialis) suhteessa GDPR:ään. GDPR kun sallii liikkumavaran käytön työoikeuden alueella.

käyttötarkoitukset, tietojen luovutettavuuden, rekisteröityjen oikeusturvan sekä henkilötietojen säilytysajat.[208] Perustuslakivaliokunta on toistanut kyseistä sääntelykohdelistaustaan satoja kertoja noin 20 vuoden ajan.[209] Tästä näkökulmasta voidaan todeta, että arkistolain (831/1994) kokonaisuudistus olisi tarpeellinen. Nykyisin viranomaisten asiakirjojen säilyttämisestä säädetään sentään lain tasolla, kun aikaisemmin tästä asiasta säädettiin muun muassa nyt jo kumotussa arkistoasetuksessa (1012/1982).

Koska sääntelyaikoja koskevan lainsäädännön tulisi olla laintasolla kattavaa ja yksityiskohtaista, olisi tällaisten säännösten määritettävä aikamääre säilytyksen kestolle.[210] Käsittelyaikoja koskevaa lainsäädäntöä on kuitenkin valitettavan vähän Suomessa ja sekin lainsäädäntö on ollut harvoin perustuslakivaliokunnan edellyttämällä tavalla lakitasoista.[211] On selvää, että vaatimus säätää tietosuojasta lailla koskee myös niitä käsittelytilanteita, joissa yksityinen sektori velvoitetaan suorittamaan tietynsisältöistä henkilötietojen käsittelyä. Näin ollen aina kun rekisterinpitäjän ainoana käsittelyperusteena on lakisääteinen velvoite, tulisi laissa määritellä myös henkilötietojen säilytysaika aikamääreen tarkkuudella näitä käsittelytilanteita varten.[212]

Kuten todettu, henkilötietojen käyttötarkoitus on olennaisessa osassa säilytyksen rajoittamisen periaatetta laajuutta arvioitaessa. Niinpä käsittelyn perustuessa GDPR:n 6(1)(b) artiklan mukaisesti sopimuksen täytäntöönpanoon, missä rekisteröity on osapuolena, tai tällaisen sopimuksen tekemistä edeltävien toimenpiteiden toteuttamiseen rekisteröidyn pyynnöstä, säilytysajan määrittäminen on hyvin selkeää. Tällöin henkilötietojen käsittelyaika on määritettävissä suoraan sopimusvelvoitteista käsin, mikäli muita käsittelyperusteita ei ole sovellettavissa. Jos käsittely perustuu GDPR:n 6(1)(a) mukaiseen suostumukseen, säilytysaika määräytyy suostumuksen kohteena olevan henkilötietojen

---

[208] PeVL 25/1998 vp, s. 2.
[209] Voutilainen 2018, s. 20.
[210] PeVL 20/2006 vp, s. 3: *”Säilytysaikaa koskevan sääntelyn tulee lain tasolla olla kattavaa ja yksityiskohtaista. Säännöstä on siten syytä täydentää aikamääreellä.”* Ks. myös PeVL 51/2002 vp, s. 2—3 sekä PeVL 25/2005 vp, s. 5—6, joissa todetaan saman suuntaisesti.
[211] Voutilainen 2018, s. 20.
[212] Henkilötietojen säilyttämistä koskevana johtopäätöksenä voidaan todeta, että julkisen vallan käyttämisestä johtuvien tai niihin liittyvien henkilörekisterien henkilötietojen säilytysajat olisi määriteltävä lakitasoisesti aikamääreiden tarkkuudella arkistolaissa (831/1994) taikka muussa lakitasoisessa erityslainsäädännössä. Asetuksen tasoinen sääntely ei ole riittävää. Samoin yksityisen sektorin toimijoiden käsitellessä henkilötietoja lakisääteiseen velvoitteeseen perustuvalla oikeusperusteella, tulisi samassa säädöksessä tai muussa erityislainsäädännössä määritellä aikamääreiden tarkkuudella henkilötietojen säilytysajat, mikäli niitä ei ole muulla tavoin lakisääteisestä velvoitteesta johdettavissa. Muiden käsittelyä koskevien oikeusperusteiden osalta yksityisellä sektorilla voidaan hyödyntää esimerkiksi Liikearkistoyhdistyksen yksityistä sektoria koskevana itsesääntelynä muodostamaa ”*Asiakirjojen säilytysajat*” -ohjeistusta, johon on listattu useimpien yksityisellä sektorilla käsiteltävien asiakirjojen säilytysajat. Ohje on *soft law* -tasoista ohjausta ja näin ollen on mahdollista, että se tulee huomioiduksi myös tietosuojaviranomaisen yksityistä sektoria koskevassa ratkaisukäytännössä sallittuna lähteenä. Viimeksi päivitetty versio asiakirjojen säilytysajoista löytyy teoksen Säilyykö sähköinen – ja kuinka kauan?, artikkelista Asiakirjojen säilytysajat, Roos 2018. Ohjeeseen on listattu säilytysaikoja myös lakisääteisten velvoitteiden nojalla tapahtuvan käsittelyn osalta. Tällöin viitatun lainsäädännön voimassaolo on tarkistettava. Esimerkiksi siinä usein viitattu henkilötietolaki ei ole enää voimassaolevaa oikeutta. Myös edelleen voimassaolevan lain säännöksiä on saatettu myöhemmin muuttaa pitämällä säädös itsessään kuitenkin voimassa.

käyttötarkoituksen perusteella. Käsittely on tällöin lopetettava myös rekisteröidyn peruuttaessa suostumuksensa[213]. Tietosuoja-asetuksen 7(3) artiklan mukaan suostumuksen peruuttaminen ei kuitenkaan vaikuta ennen sen ilmaisemista tapahtuneeseen käsittelyyn.

### 1.6. Eheys ja luottamuksellisuus (tietoturvallisuuden periaate)

Yleisen tietosuoja-asetuksen 5(1)(f) artiklan mukaan henkilötietoja *"on käsiteltävä tavalla, jolla varmistetaan henkilötietojen asianmukainen turvallisuus, mukaan lukien suojaaminen luvattomalta ja lainvastaiselta käsittelyltä sekä vahingossa tapahtuvalta häviämiseltä, tuhoutumiselta tai vahingoittumiselta käyttäen asianmukaisia teknisiä ja organisatorisia toimia"*. Toisin sanoen rekisterinpitäjän on huolehdittava henkilötietoja käsitellessään tietoturvallisuudesta asianmukaisin teknisin ja organisatorisin toimenpitein. Eheyden ja luottamuksellisuuden periaate tunnetaankin myös tietoturvallisuuden (*security*) periaatteena.[214] Edellä mainittu säännös ilmentää tietosuoja-asetuksessa omaksuttua riskilähtöistä lähestymistapaa, joka tulee esille myös edellä käsiteltyä täsmällisyysvaatimusta koskevassa säännöksessä.

Käsittelyn turvallisuutta koskevan tietosuoja-asetuksen 32(1) artiklan mukaan tietoturvallisuutta koskevassa riskiarviossa on otettava huomioon uusimmat tekniikat, toteuttamiskustannukset, käsittelyn luonne, laajuus, tarkoitus ja asiayhteys sekä yksilön oikeuksille ja vapauksille kohdistuvat, todennäköisyydeltään ja vakavuudeltaan vaihtelevat riskit. Turvallisuustoimenpiteiden olisi siis oltava oikeassa suhteessa näihin riskeihin nähden. Asianmukaisina teknisinä ja organisatorisina toimenpiteinä säännöksessä mainitaan esimerkinomaisesti

- henkilötietojen pseudonymisointi[215] ja salaus
- kyky taata käsittelyjärjestelmien ja palveluiden jatkuva luottamuksellisuus, eheys, käytettävyys ja vikasietoisuus
- kyky palauttaa nopeasti tietojen saatavuus ja pääsy tietoihin fyysisen ja teknisen vian sattuessa
- menetelmä, jolla testataan, tutkitaan ja arvioidaan säännöllisesti teknisten ja organisatoristen toimenpiteiden tehokkuutta tietojenkäsittelyn turvallisuuden varmistamiseksi.

---

[213] GDPR:n 7(3) artikla.

[214] ICO:n ohje: Principle (f): Integrity and confidentiality (security).

[215] GDPR:n 4(5) artiklan mukaan pseudonymisoimisella tarkoitetaan *"henkilötietojen käsittelemistä siten, että henkilötietoja ei voida enää yhdistää tiettyyn rekisteröityyn käyttämättä lisätietoja, edellyttäen että tällaiset lisätiedot säilytetään erillään ja niihin sovelletaan teknisiä ja organisatorisia toimenpiteitä, joilla varmistetaan, ettei henkilötietojen yhdistämistä tunnistettuun tai tunnistettavissa olevaan luonnolliseen henkilöön tapahdu"*. Tämä voidaan toteuttaa esimerkiksi siten, että toisessa tietokannassa on metatietojen avulla järjestettynä tiettyjä henkilöitä koskevia tietoja ja toisessa tietokannassa on ensiksi mainitussa tietokannassa listattuihin tietoihin metatietojen avulla yhdistettävät henkilöt luetteloituna. Pseudonymisoiminen on lisäedellytyksenä järjestettävä siten, että teknisin ja organisatorisin toimenpitein huolehditaan siitä, ettei toiseen tietokantaan luvattomasti pääsevällä taholla ole todennäköisesti pääsyä myös toisessa tietokannassa oleviin yhdistäviin tietoihin.

Näin ollen tietoturvassa on kyse sekä fyysisten että aineettomien teknisten vikojen ennaltaehkäisemisestä. Huomiota ei tule kiinnittää pelkästään ulkoisiin riskeihin vaan lisäksi organisaation sisäiset riskit, kuten järjestelmien toimivuus ja tietojen eheyden säilyminen, on otettava huomioon. Henkilöiden pääsyä tietoihin on rajoitettava myös organisaation sisällä siten, että ainoastaan sellaisilla henkilöillä on pääsy tietoihin, joiden työtehtäviin kuuluu kyseisten henkilötietojen käsittely. Koska arvio tehdään riskiperusteisesti, tulee muun muassa henkilötietojen erityisryhmiin kuuluvien tietojen osalta noudattaa erityistä tarkkaavaisuutta.[216] Säännöllisellä teknisten ja organisatoristen toimenpiteiden arvioinnilla tarkoitetaan myös jälkikäteistä auditointia, johon palataan tutkielman III osan jälkivalvontaa koskevassa 4.6. luvussa. Ennakkovalvontaa koskevassa 4.1.2. luvussa etenkin riskilähtöinen lähestymistapa on käsittelyn kohteena.

Tietosuoja-asetuksen 32(2) artiklan perusteella asianmukaisen turvallisuustason arvioimisessa on kiinnitettävä huomiota erityisesti käsittelyn sisältämiin riskeihin, kuten siirrettyjen tietojen laittoman tai vahingossa tapahtuvan tuhoamisen, muuttamisen, luvattoman luovuttamisen, pääsyn ja häviämisen muodossa tapahtuviin tilanteisiin. Tietosuoja-asetuksen 32(3) artiklassa mainittuja vaihtoehtoisia keinoja tietoturvallisuuden takaamiseksi ovat GDPR:n 40 artiklassa tarkoitettu hyväksyttyjen käytännesääntöjen käyttöön ottaminen ja GDPR:n 42 artiklassa tarkoitettu sertifiointimekanismien hyödyntäminen. Näkemykseni mukaan nimenomaan merkittäviä tietoturvaan kohdistuvia riskejä sisältävissä käsittelyprosesseissa käytännesääntöjen ja sertifiointimekanismien käyttöönottamista tulisi erityisesti harkita. Näiden toimenpiteiden osalta kyse ei kuitenkaan ole niin sanotusti pakottavista toimista, vaan niiden käyttöönottaminen on jätetty täysimääräisesti rekisterinpitäjän harkittavaksi. Tällöin niiden funktiona on erityisesti tietosuojaperiaatteiden noudattamisen helpottaminen esimerkiksi varmuudella tietosuoja-asetuksen mukaisen vaatimustason täyttäviä hyväksyttyjä käytännesääntöjä noudattamalla.

Tietosuoja-asetuksen 32(4) artiklassa puolestaan todetaan, että henkilötietojen käsittelijän ja rekisterinpitäjän on kumpaisenkin varmistettava, että heidän alaisuudessaan toimivat henkilötietoja käsittelevät yksilöt käsittelevät tietoja ainoastaan rekisterinpitäjän antamien ohjeiden mukaisesti. Tämä ilmentää sitä, että nimenomaisesti rekisterinpitäjällä on velvollisuus antaa henkilötietojen käsittelyä koskevat ohjeet, joissa on otettava huomioon riittävässä määrin tietoturvallisuuden varmistaminen. Nämä ohjeet sitovat myös organisaatioita, jotka toimivat henkilötietojen käsittelijän ominaisuudessa. Näin ollen *tietojenkäsittelysopimuksen* on sisällettävä tietoturvallisuutta koskevia toimenpiteitä määrittävät toimintaohjeet, jotka ovat todennäköisesti luontevinta sisällyttää tietojenkä-

[216] ICO:n ohje: Security.

sittelysopimuksen liitteeseen. Tällaiset ohjeet on nähtävissä tarpeen mukaan päivittyvinä asiakirjoina, muun muassa auditoinneissa havaittujen puutteiden tai riskitason mahdollisen kasvamisen perusteella.

Tietoturvan keskeisimpänä tavoitteena on turvata tietojen eheys, luottamuksellisuus ja käytettävyys. Tästä johtopäätöksenä tietoturvariskeillä tarkoitetaan ei-toivottuja tilanteita, joissa tietoturvan edellä mainitut elementit vaarantuvat.[217] Aktualisoitunut tietoturvariski voi olla luonteeltaan tahallisesti, tahattomasti tai oikeudettomasti aiheutettu vahinko. Tietoturvavahingot ovat yleensä luonteeltaan taloudellisia, aiheuttaen liiketoiminnan keskeytymistä, aineettomien oikeuksien loukkauksia sekä vahinkoon liittyviä tutkinta- ja suojautumistoimia. Riskit aktualisoituvat yleensä teknisistä suunnittelu-, toiminta- ja sopimussuhdevirheistä sekä lisäksi liiketoiminnasta korkean tietoturvariskin omaavissa valtioissa.[218]

Riski merkitsee tietyn uhan aiheuttaman vahingon tai menetyksen todennäköisyyttä.[219] Direktiivin (EU) 1148/2016[220] (*Verkko- ja tietojärjestelmädirektiivi)* 4(9) artiklassa täsmennetään, että riskillä tarkoitetaan *”mitä tahansa kohtuullisesti tunnistettavissa olevaa tilannetta tai tapahtumaa, joka saattaa vaikuttaa haitallisesti verkko- ja tietojärjestelmien turvallisuuteen”*. Tietosuojakontekstissa kyse on yksityisyyden suojalle kohdistuvista riskeistä henkilötietojen käsittelyssä.[221] Tässä mielessä yleisen tietosuoja-asetuksen tarkoittamista tietoturvariskeistä suojauduttaessa, arvioitavaksi ei tule niinkään rekisterinpitäjälle mahdollisesti koituvat vahingot ja menetykset, kuten mainehaitta, vaikka todennäköisesti yksilöille aiheutuva vahinko tulee vaikuttamaan myös yhtiön maineeseen. Riskilähtöisellä lähestymistavalla tarkoitetaankin GDPR:ssä ennen kaikkea yksilölle aiheutuvien riskien arvioimista. Tietoturvallisuuden periaate velvoittaa siis henkilötietojen eheyden ja luottamuksellisuuden varmistamista riskiperusteisen lähestymistavan pohjalta toteutetuin toimenpitein.

---

[217] Valtioneuvoston periaatepäätös, 24.1.2013, s. 13. On syytä huomata, ette ”*-päätös*” loppuliitteestä huolimatta valtioneuvoston periaatepäätökset eivät ole sitovia oikeuslähteitä, vaan niillä on ennen kaikkea suositusluontoinen ohjaava vaikutus.

[218] Liikenne- ja viestintäministeriö, 4/2016, s. 15.

[219] VAHTI, 7/2003, s. 77.

[220] Verkko- ja tietojärjestelmädirektiivin 1(1) artiklan mukaan se on säädetty korkeatasoisen verkko- ja tietojärjestelmien turvallisuuden takaamiseksi unionin sisämarkkinoilla. Kyseinen säädös on ns. yleislaki tietoturvallisuuden alueella, joten esimerkiksi asetuksen (EU) N:o 910/2014 19 artiklan mukaiset turvallisuus- ja ilmoitusvaatimuksia koskevat tarkentavat säännökset syrjäyttävät verkko- ja tietojärjestelmädirektiivin yleisluonteisemmat säännökset luottamuspalveluiden tarjoajien osalta. On myös huomattava, että direktiivin tarkoituksena ei ole tietoturvaoikeudellisena instrumenttina ylläpitää ainoastaan henkilötietojen suojaa, vaan kyse on myös esimerkiksi liikesalaisuuksien suojaamisesta (ks. esim. verkko- ja tietojärjestelmädirektiivin 1(5) artikla). Verkko- ja tietojärjestelmädirektiivillä on vaikutusta niin yksityisen kuin julkisenkin sektorin toimijoihin sen soveltamisalalla.

[221] VAHTI, 1/2016, s. 12.

## 2. Osoitusvelvollisuuden suhde muihin tietosuojaperiaatteisiin

Osoitusvelvollisuutta voidaan pitää yleisen tietosuoja-asetuksen myötä uutena tietosuojalainsäädännön perusperiaatteena.[222] Osoitusvelvollisuuden sisällyttäminen tietosuoja-asetukseen on ratkaisu jo aikaisemmin oikeuskirjallisuudessa esille tuotuun tarpeeseen saada tehokkaampia takeita henkilötietojen suojan toteutumiseksi.[223] Lainsäätäjän rationaalisuuden olettama johtaa siihen, että tietosuojaperiaatteiden ollessa määriteltynä tietosuoja-asetuksen 5(1) artiklassa, mutta osoitusvelvollisuuden ollessa määritelty tietosuoja-asetuksen 5(2) artiklassa ja kun sen soveltaminen on rajattu ainoastaan rekisterinpitäjään, niin tietosuojaperiaatteita tulee tämän perusteella noudattaa jokaisen henkilötietojen käsittelyyn osallistuvan. Kuitenkin vastuu tietosuojaperiaatteiden toteutumisen osoittamisesta on vain rekisterinpitäjällä.[224] Toisin sanoen lainsäätäjällä on tullut olla tarkoitus erottaa ainoastaan rekisterinpitäjään sovellettava osoitusvelvollisuus muista tietosuojaperiaatteista, joiden yhteydessä sovellettavuutta ei ole erikseen rajoitettu ainoastaan rekisterinpitäjään.[225]

*Rekisterinpitäjä* on yleisen tietosuoja-asetuksen 4(7) artiklan mukaan luonnollinen tai oikeushenkilö, virasto, viranomainen tai muu elin, joka yksin tai yhdessä toisten kanssa määrittelee henkilötietojen käsittelyn tarkoituksen sekä keinot. Ilmaisulla ”muu elin” tarkoitetaan sitä, että käytännössä ei ole millään tavalla rajoitettu sitä, millainen taho voi olla rekisterinpitäjä.[226] Määritelmän voi todeta sisältävän samat kolme ainesosaa kuin aikaisempi henkilötietodirektiivi eli ensinnäkin rekisterinpitäjä voi olla mikä tahansa organisaatio tai henkilö, toiseksi rekisterinpitäjänä voi toimia yksin tai yhdessä muiden kanssa ja kolmanneksi rekisterinpitäjä määrittelee käsittelyn tarkoituksen ja keinot.[227] Määritelmä johtaakin yhdessä tietosuoja-asetuksen yhteisrekisterinpitäjää koskevan 26 artiklan kanssa siihen, että samanaikaisesti voi olla myös useampi osapuoli osoitusvelvollisuuden alainen samasta käsittelystä.[228]

Osoitusvelvollisuus jakautuu kahteen elementtiin. Ensinäkin, rekisterinpitäjän vastuuseen kyetä osoittamaan tietosuojaperiaatteiden toteutuminen ja toiseksi, velvollisuuteen noudattaa tietosuojaperiaatteita. Näitä elementtejä voidaan tarkastella yhdessä tietosuoja-asetuksen 24(1) artiklassa määritellyn rekisterinpitäjän vastuun kanssa. Sen mukaan rekisterinpitäjän tulee toteuttaa riittävät tekniset ja organisatoriset toimenpiteet, joilla voidaan varmistaa ja osoittaa, että käsittelyssä noudatetaan tietosuojalainsäädäntöä. Tämä herättääkin mielenkiintoisen kysymyksen siitä, mihin lopulta osoitusvelvollisuus rajoittuu. Sanamuodon mukaisella tulkinnalla voidaan päätyä siihen, että osoi-

[222] Buttarelli 2017, s. 1.
[223] Tzanou 2017, s. 62.
[224] Ks. esim. Lynskey 2015, s. 35, “*The assumption of rationality of the legislator”.*
[225] Tietosuojavaltuutetun toimiston ohje: Osoita noudattavasi tietosuojalainsäädäntöä.
[226] Van Alsenoy 2016a, s. 44.
[227] Tietosuojatyöryhmä, WP 250, s. 7—8.
[228] Voigt et al. 2017, s. 34.

tusvelvollisuus kohdistuu ainoastaan tietosuoja-asetuksen 5(1) artiklassa mainittuihin tietosuojaperiaatteisiin. Tietosuoja-asetuksen 24 artiklassa on kuitenkin edellä kuvatulla tavalla käytetty käsitettä ”*osoittaa*”, jolloin voidaan perustellusti päätyä siihen, että rekisterinpitäjän tulee kyetä riittävin teknisin ja organisatorisin toimenpitein osoittamaan, että tämä noudattaa kaikkia toiminnassaan relevantteja yleisen tietosuoja-asetuksen asettamia vaatimuksia.[229] Näin ollen on perusteltua ajatella, että pohjimmiltaan tietosuoja-asetuksen säännökset ilmentävän GDPR:n 5(1) artiklassa mainittuja tietosuojaperiaatteita.[230]

Merkityksellistä on myös se, kenelle rekisterinpitäjän tulee pystyä osoitusvelvollisuuden mukaisesti osoittamaan toimivansa tietosuojaperiaatteiden mukaisesti. Tietosuojatyöryhmä on antanut vastauksen tähän kysymykseen ja todennut, että tietosuojaperiaatteiden noudattaminen tulee osoittaa tietosuojaviranomaiselle, jolla on mahdollisuus määrätä hallinnollisia sakkoja.[231] Osoitusvelvollisuudesta johtuen *tietosuojaviranomaisella* on siis oikeus saada tietoja rekisterinpitäjältä. Näillä tiedoilla tarkoitetaan näyttöä siitä, että rekisterinpitäjä noudattaa tietosuojaperiaatteita ja -velvoitteita. Edellä mainittu pitää sisällään dokumentaation täytäntöönpanotoimista, joilla varmistetaan tietosuojavelvoitteiden noudattaminen sekä osoitetaan riittävän vaatimustason noudattamisen omatoiminen valvonta.[232]

### 3. Henkilötietojen käsittelyn oikeusperuste

Henkilötietojen käsittelylle on aina oltava jokin yleisen tietosuoja-asetuksen 6 artiklassa määritelty oikeusperuste. Nämä oikeusperusteet vastaavat pitkälti henkilötietodirektiiviin perustuneita oikeusperusteita.[233] Jos henkilötietojen käsittely ulkoistetaan rekisterinpitäjän toimesta toiselle organisaatiolle, toimii tämä henkilötietojen käsittelijä käsittelytoimissaan rekisterinpitäjän oikeusperusteen nojalla.[234] Mikäli käsittely kohdistuu *erityisiin henkilötietoryhmiin*, tulee tietosuoja-asetuksen 6 artiklassa säädetyn oikeusperusteen[235] täyttymisen lisäksi täyttyä jokin tietosuoja-asetuksen 9 artiklassa säädetty peruste.[236] Toisin sanoen erityisiin henkilötietoryhmiin kuuluvien tietojen käsitteleminen on lähtökohtaisesti kielletty, mutta näiden tietojen käsittely on poikkeuksellisesti sallittua asetuksen 9 artiklassa määritellyin perustein. Näin ollen rekisterinpitäjän on erityisen tärkeää pystyä

---

[229] Ks. de Hert s. 198.
[230] Ks. Euroopan tietosuojaneuvosto: Annex to Opinion 3/2015, Article 5 ja 22.
[231] Article 29 Data Protection Working Party, WP 250, s. 19.
[232] Article 29 Data Protection Working Party, WP 173, kohdat 59—60.
[233] TATTI-mietintö 35/2017, s. 21.
[234] Ks. Article 29 Data Protection Working Party, WP 169, s. 14, siitä kenen näkökulmasta oikeusperusteen täyttymistä arvioidaan.
[235] Yleisiä käsittelyn oikeusperusteita ovat GDPR:n 6(1) artiklan nojalla rekisteröidyn antama suostumus, sellaisen sopimuksen täytäntöönpaneminen tai laatiminen, jonka osapuolena rekisteröity olisi, rekisterinpitäjän lakisääteinen velvollisuus, rekisteröidyn tai toisen luonnollisen henkilön elintärkeiden etujen suojeleminen, rekisterinpitäjän taikka toisen rekisterinpitäjän oikeutettu etu ja rekisterinpitäjälle kuuluvan julkisen vallan käyttäminen tai yleisen edun nojalla suoritettavan tehtävän toteuttaminen.
[236] HE 9/2018 vp, s. 122.

tunnistamaan, millä perusteella tämä käsittelee henkilötietoja, jotta tietosuoja-asetuksen noudattaminen on mahdollista.[237] Tämän takia myös ulkoistamisen yhteydessä olisi tärkeää, että oikeudellinen asiakirja, joka solmitaan henkilötietojen käsittelijän kanssa, sisältäisi tiedot siitä, millä oikeusperusteilla tietoja tullaan käsittelemään. Tällöin myös henkilötietojen joukko tulee asiallisesti rajatuksi riittävän suppeaksi.

On huomioitava, että mikäli oikeusperusteena on *suostumus*, vastaa lähtökohtaisesti rekisterinpitäjä siitä, että tämän henkilötietojen käsittelijälle mahdollisesti luovuttamiensa henkilötietojen käsittelylle on annettu suostumus rekisteröidyn toimesta. Suostumuksen tulee olla vapaaehtoinen, yksilöity, tietoinen sekä yksiselitteinen, mutta se voi kuitenkin olla sähköisen tai kirjallisen muodon lisäksi suullinen.[238] Joka tapauksessa tietosuoja-asetuksen 7(1) artiklan mukaan rekisterinpitäjällä on näyttötaakka suostumuksesta eli olennaista on se, että rekisterinpitäjä kykenee näyttämään, että suostumus on annettu. Suostumuksen tulee olla sitoumusluontoinen eikä sopimuksen muodossa, sillä siinä missä sopimus asettaa osapuolille velvoitteen noudattaa sopimusvelvoitteita, niin sitoumus on yksipuolisesti peruutettavissa milloin tahansa niin kuin tietosuoja-asetus edellyttää. Kuten todettu, suostumuksen tulee olla tietoinen, yksilöity ja yksiselitteinen. Toisin sanoen, jotta suostumus kattaisi jokaisen käsittelytarkoituksen, on suostumuspyyntöön sisällyttävä kaikki käsittelytarkoitukset selkeässä ja tiiviissä muodossa.[239] Näiden seikkojen täyttymisen osoittaminen on osa rekisterinpitäjän osoitusvelvollisuutta.[240]

On syytä huomata, että mikäli rekisteröity on lapsi, tietosuoja-asetuksen mukaan suostumusta on tällöin pyydettävä myös lapsesta vanhempainvastuuta kantavalta, kun kyse on tietoyhteiskunnan palvelun tarjoamisesta. GDPR:n 8 artiklan mukaan lapsi on määritelty alle 16-vuotiaaksi, mutta se voidaan kansallisessa lainsäädännössä asetuksesta poiketen määritellä liikkumavaran johdosta vähintään 13-vuotiaaksi. Tietosuojalain 5 §:n mukaisesti Suomessa ikärajaksi on säädetty 13 vuotta.[241]

Myös henkilötietodirektiivi sisälsi oikeusperusteen käsitellä henkilötietoja, kun kyse on rekisterinpitäjän tai kolmannen osapuolen *oikeutettua etua* koskevasta henkilötietojen käsittelystä. Henkilötietolaissa tarkennettiin kyseistä oikeusperustetta. Henkilötietolain mukaan tietosuojalautakunta on voinut myöntää luvan edellä mainitulla oikeusperusteella käsitellä henkilötietoja. Yleinen tietosuoja-asetus muutti tilannetta kuitenkin siten, että jatkossa tietosuojalautakunnalla[242] ei ole tällaista toimivaltaa ja vastuu rekisterinpitäjän tai kolmannen osapuolen oikeutetun edun edellytyksen täyttymisen arvioinnista siirtyy täysimääräisesti rekisterinpitäjälle. Tässä kohden on syytä mainita, että

[237] Oikeusministeriön selvityksiä ja ohjeita, 4/2017, s. 19.
[238] Ibid. s. 20.
[239] Ks. esim. Salokannel 2016, s. 540, toteaa saman suuntaisesti.
[240] Oikeusministeriön selvityksiä ja ohjeita, 4/2017, s. 20.
[241] HE 9/2018 vp, s. 54.
[242] Tietosuojalautakunnan toiminta lakkautettiin Suomessa GDPR:n myötä.

oikeutettu etu ei aina syrjäytä rekisteröityjen etuja tai perusoikeuksia ja tällainen tilanne voi olla käsillä, jos rekisteröity on esimerkiksi lapsi.[243]

### 4. Osoitusvelvollisuus käytännössä

Jotta osoitusvelvollisuus voidaan täyttää, on organisaation ensin kyettävä hahmottamaan henkilötietojen käsittelylle olemassa olevat prosessit.[244] Kyse on pohjimmiltaan riskienhallinnasta, joten on erityisen tärkeää ymmärtää, mihin prosessin vaiheisiin sisältyy suurimpia riskejä.[245] Yksi keino kartoituksen tekemiseksi on suorittaa *tietotilinpäätös*, joka laaditaan organisaation sisäisen auditoinnin tuloksena, ja joka kohdistuu henkilötietojen käsittelyn keskeisiin asioihin.[246] Kun organisaation henkilötietojen käsittelyyn liittyvät käytännöt on selvitetty, tulee arvioida täyttävätkö organisaation sen hetkiset käytännöt tietosuoja-asetuksen sekä sen nojalla säädetyn kansallisen lainsäädännön asettamat vaatimukset.[247]

Lähtökohtana rekisterinpitäjän velvoitteiden arvioinnissa on *riskiperusteinen lähestymistapa*, jonka vuoksi rekisterinpitäjän tulee kartoittaa edellä kuvatulla tavalla käsittelyn rekisteröidyn oikeuksille ja vapauksille muodostamat riskit sekä varautua niihin riittävin tietosuoja-asetuksen mukaisin toimenpitein.[248] Näiden vaadittujen toimenpiteiden laajuus sekä laatu puolestaan riippuu käsiteltävien henkilötietojen tyypistä sekä käsittelyyn liittyvän riskin suuruudesta.[249] Riskinä voidaan pitää kaikkia aineellisia tai aineettomia vahinkoja, jotka rekisteröidylle voi henkilötietojen käsittelyn seurauksena muodostua.[250] Näin ollen riskitaso kasvaa, kun käsitellään suuria määriä tietoja tai henkilöitä profiloidaan[251] heidän ominaisuuksiaan analysoimalla taikka käsiteltävät henkilötiedot koostuvat henkilötietojen erityisryhmistä.

On syytä painottaa rekisterinpitäjän olevan vastuussa siitä, että tietosuojaperiaatteita noudatetaan kaikissa henkilötietojen käsittelyn vaiheissa, myös henkilötietojen käsittelyn ulkoistustilanteissa. Näin ollen rekisterinpitäjän on arvioitava näiden periaatteiden sisältö ja määriteltävä ne keinot, joilla kyseiset periaatteet ovat täytettävissä sen toiminnassa. Osoitusvelvollisuuden täyttäminen edellyttää käytännössä aiempaa tarkempaa suunnittelua sekä dokumentointia käsittelytoimista.[252]

---

[243] Oikeusministeriön selvityksiä ja ohjeita, 4/2017, s. 19—20.
[244] Ibid. s. 11.
[245] Ibid. s. 14.
[246] Ibid. s. 11.
[247] TATTI-mietintö 35/2017, s. 127; Ks. myös tutkielman Liite 1.
[248] Salokannel 2016, s. 538.
[249] Ibid. s. 538.
[250] Ks. esim. Salokannel 2016, s. 538, toteaa saman suuntaisesti.
[251] Alén-Savikko 2017, s. 107.
[252] Oikeusministeriön selvityksiä ja ohjeita, 4/2017, s. 12.

Tulkinta-apua tietosuojaperiaatteiden arvioimiseen tuo yleisen tietosuoja-asetuksen johdanto-osan 39 kappale,[253] jonka mukaan henkilötietojen käsittelyn tulee olla *laillista ja asianmukaista*. Kohdassa todetaan myös, että *läpinäkyvyydellä* tarkoitetaan sitä, että luonnollinen henkilö voi halutessaan olla tietoinen siitä, miten häntä koskevia henkilötietoja kerätään ja käytetään sekä muulla tavoin käsitellään. Lisäksi rekisteröidyllä on oikeus tietää käsittelyn tarkoitus ja kuinka laajamittaisesti henkilötietoja on määrä käsitellä. Tämä johtaa luonnollisesti siihen, että tarpeellisten tietojen on oltava helposti saatavilla sekä ymmärrettävissä, ja jotta läpinäkyvyyden periaate ei jäisi tyhjäksi, on myös huolehdittava, että annetussa informaatiossa on käytetty selkeää ja ymmärrettävää kieltä. GDPR:n johdanto-osan 39 kappaleen mukaan edellä mainittu koskee erityisesti tietoja rekisterinpitäjän identiteetistä ja henkilötietojen käsittelyn tarkoituksista sekä niitä lisätietoja, jotka ovat tarpeellisia varmistettaessa käsittelyn asianmukaisuus ja läpinäkyvyys.

Tietosuoja-asetuksen johdanto-osan 39 kappaleessa myös todetaan, että luonnollisen henkilön tulee pystyä tiedostamaan käsittelyyn liittyvät riskit sekä säännöt, joita tulee noudattaa käsittelyssä. Lisäksi käytetyt suojatoimet sekä rekisteröidyn oikeudet ja ohjeistus, miten nämä oikeudet ovat toteutettavissa, tulee käydä helposti havaittavalla tavalla ilmi. Oikeuksien toteuttamisesta ei tule tehdä liian hankalaa ja näin ollen *selkeyden vaatimus* ilmenee monesta muustakin tietosuoja-asetuksen kohdasta. Esimerkiksi asetuksen rekisteröidyn suostumusta koskevassa 7(2) artiklassa todetaan, että suostumuksen antamista koskevan pyynnön tulee olla selkeä ja kieleltään yksinkertainen sekä sen on oltava selvästi erillään muista asioista.

Usein on kysytty, kuinka tarkkoja annettujen tietojen tulee olla esimerkiksi koskien henkilötietojen käsittelyn tarkoitusta, kun monesti nämä tarkoitukset voivat olla hyvinkin moninaisia. Tähänkin löytyy vastaus tietosuoja-asetuksen johdanto-osan 39 kappaleesta, jonka mukaan erityisesti käsittelyn nimenomaisen tarkoituksen on käytävä ilmi ja nämä tiedot tulee ilmoittaa jo henkilötietojen keräämisen yhteydessä. Rekisterinpitäjän vastuulle jää tietenkin arvioitavaksi se, että nämä nimenomaiset tarkoitukset ovat yhdenmukaisia kerättyjen tietojen kanssa eli toisin sanoen, että näitä tietoja kerätään riittävästi ja tiedot ovat olennaisia tarkoitusten toteuttamisen kannalta. Lisäksi kerättyjen tietojen on rajoituttava siihen, mikä on välttämätöntä etukäteen määritellyn tarkoituksen toteuttamiseksi.

Koska rekisterinpitäjän tulee osoittaa noudattavansa tietosuojaperiaatteita koko tiedon elinkaaren ajan, on henkilötietojen säilyttämisaikojen oltava mahdollisimman lyhyitä. Käsittelyn tarkoituksen ja käsittelytoimien välinen suhde näkyy myös siten, että henkilötietojen käsittelyyn tulisi ryhtyä vain, mikäli tarkoitusta ei ole kohtuudella toteutettavissa muilla keinoin. Suunnitelmallisuus ulottuu

[253] Oikeusministeriön selvityksiä ja ohjeita, 4/2017, s. 12.

siis tiedon koko elinkaareen ja toisaalta käytettävät tietojärjestelmät on valittava ja suunniteltava ainoastaan tarpeellisten tietojen hyödyntämistä varten.[254]

Osoitusvelvollisuuden täyttäminen edellyttää siis tietosuoja-asetuksen johdanto-osan mukaan konkreettisten henkilötietojen säilytysaikojen määrittelemistä ja toisaalta näiden määräaikojen tarkastelemista käsittelyn tarkoituksen valossa tietyin väliajoin. Kun henkilötietoja ei ole enää tarpeellista säilyttää, tulee ne luonnollisesti poistaa järjestelmästä tai anonymisoida. Tähän liittyy myös kohtuullisten toimenpiteiden toteuttaminen sen varmistamiseksi, että virheelliset henkilötiedot oikaistaan tai poistetaan. Toisin sanoen järjestelmän ei tule olla sellainen, että tietojen oikeellisuus on ainoastaan sen varassa, että rekisteröity joskus vaatii virheellisten tietojen oikaisemista tietosuoja-asetuksen 16 artiklan mukaisesti, vaan tietojen oikeellisuutta on arvioitava tietyin väliajoin ja siinä määrin, mitä voidaan kohtuudella rekisterinpitäjältä edellyttää. Tähän puolestaan vaikuttaa teknologinen kehitys, joka mahdollistaa yhä parempia keinoja edellä mainittujen toimenpiteiden toteuttamiseksi.

Edellä kuvattuja toimenpiteitä arvioitaessa on huomioitava myös yleisen tietosuoja-asetuksen 25 artikla, jossa on määritelty oletusarvoinen tietosuoja. Sen mukaisesti rekisterinpitäjän on huolehdittava tarpeellisin teknisin ja organisatorisin toimenpitein siitä, että oletusarvoisesti käsitellään ainoastaan käsittelyn tarkoituksen kannalta tarpeellisia tietoja. Tietosuoja-asetuksen 25 artiklassa edellytetään myös sisäänrakennettua tietosuojaa, jossa on huomioitu uusimmat tekniikat ja niiden toteutuskustannukset. Kohtuullisia tietosuojakustannuksia voidaan pitää aina sitä korkeampina, mitä suuremmista riskeistä on kyse, huomioiden muun muassa käsittelyn luonne sekä laajuus.[255]

Näin ollen käytännön tasolla osoitusvelvollisuuden voidaan ajatella jakautuvan neljään osaan. Ensinnäkin organisaatiolla tulee olla sen ylimmän johdon suosittelemat ja hyväksymät läpinäkyvät tietosuojaperiaatteet. Toiseksi, kaikkien organisaatiossa toimivien henkilöiden tulee olla tietoisia näistä tietosuojaperiaatteista ja heille on annettava tarpeellinen koulutus periaatteiden noudattamiseksi. Kolmanneksi, organisaation korkeimmalle tasolle tulee kohdentua vastuu tietosuojaperiaatteiden noudattamisesta. Vastuu johtaa korkeimman johdon tarpeeseen arvioida tietyin väliajoin tietosuojaperiaatteiden noudattamisen tasoa. Vastuu johtaa myös korkeimman johdon velvollisuuteen pystyä näyttämään yhteistyökumppaneille ja tietosuojaviranomaiselle sekä muille asianomai-

[254] Saarenpää 2015, s. 356—357.
[255] Ks. esim. Salokannel 2016, s. 538—539, kohtuullisista tietosuojatoimenpiteistä.

sille riittävän tietosuojatason toteutuminen. Neljänneksi, organisaatiolla tulee olla käytössään protokollat, joita noudattaen voidaan puuttua puutteelliseen tietosuojaperiaatteiden noudattamiseen sekä tietosuojaloukkauksiin[256].[257]

### 4.1. Riskiperusteinen lähestymistapa

Riskienhallinta on kaikkea sellaista toimintaa, jolla pyritään välttämään toiminnassa mahdollisesti olevia riskejä sekä niistä johtuvia vahinkoja.[258] Riskienhallinnassa on tarkoitus ensin tunnistaa ja seuraavaksi hallita organisaation toimintaa haittaavia ja vahingoittavia tekijöitä sekä välttää näiden tapahtumien aktualisoitumista ja pienentää niistä aiheutuvia seurauksia pitäen riskit sellaisella tasolla, ettei organisaation toiminta ja siihen liittyvät tavoitteet ole uhattuna.[259] Riskienhallintaan kuuluu siis olennaisena osana riskien arvioiminen, jolla pyritään tunnistamaan uhkia sekä haavoittuvuuksia jo ennen niiden mahdollista aktualisoitumista. Arvioinnin avulla tapahtuvan tietoturvan kehitystyön tulisi olla jatkuvaa ja riskienhallintaan kuuluvaa riskien arviointia olisi tehtävä säännöllisesti.[260]

Kuten aikaisemmin on todettu, riskienhallintaa edellyttäviä tietosuojaperiaatteita ovat tietosuoja-asetuksen sanamuodon perusteella täsmällisyysperiaate sekä eheys ja luottamuksellisuus (*tietoturvallisuuden periaate*). Myös GDPR:n johdanto-osan profilointia ja automatisoitua päätöksentekoa koskevassa 71 kappaleessa edellytetään riskienhallintaa nimenomaisesti virheriskin mitigoimisen eli minimoimisen muodossa, joka on itseasiassa toimeksianto käyttää ainakin kyseistä riskinhallintakeinoa. Edellä mainitussa kohdassa on kuitenkin kyse pohjimmiltaan *täsmällisyyden* ja *tietoturvallisuuden periaatteen* noudattamisesta.

Yleisessä tietosuoja-asetuksessa omaksutun riskiperusteisen lähestymistavan[261] mukainen riskienhallinta voi koostua useista erilaisista riskienhallintakeinoista eli tavoista, joilla riskeihin reagoidaan ennen niiden aktualisoitumista. Ensimmäisenä vaiheena on tunnistaa tietojenkäsittelyyn liittyvät uhat. Kun uhka on tunnistettu, tulee arvioida sen todennäköisyys ja aktualisoituneen riskin

---

[256] Tietosuojaloukkaus on tietoturvaloukkausta laajempi käsite ja se tarkoittaa kaikkea tietosuojalainsäädännön vastaista toimintaa tai laiminlyöntiä. Tietoturvaloukkaus on puolestaan määritelty erikseen GDPR:n 4 artiklan 12-kohdassa ja sellaisen tapahduttua, tulee tehdä ilmoitus tietosuojaviranomaiselle 72 tunnin kuluessa tietoturvaloukkauksen havaitsemisesta, ja korkean riskin käsillä ollessa ilmoitus tulee tehdä myös rekisteröidyille. Tietoturvaloukkaus sisältyy tietosuojaloukkauksen käsitteen alaan.

[257] European Data Protection Supervisor, 7.6.2016. Ks. myös tutkielman liite 1: Prosessikaavio osoitusvelvollisuuden toteuttamiseksi.

[258] Andersson 2018, s. 3.

[259] Katakri 2015, s. 8—9.

[260] Ks. esim. VAHTI, 1/2016, s. 12, liittyen riskien tarkasteluun yksilön henkilötietojen suojan näkökulmasta; VAHTI, 7/2003, s. 4, 15 ja 18, riskienhallintaan liittyvän arvioinnin säännöllisyydestä.

[261] Lähes kaikessa yleistä tietosuoja-asetusta käsittelevässä oikeuskirjallisuudessa todetaan, että GDPR:n lähtökohtana on riskilähtöisyys tai riskiperusteinen lähestymistapa. Ks. esim. Andersson 2018, s. 6. Riskilähtöisyyttä tai riskiperusteisuutta ei kuitenkaan mainita GDPR:ssä tai sen johdanto-osassa erikseen. On silti selvä asia, että tietosuoja-asetuksen toimeksiannoissa suorittaa riskien kannalta asianmukaisia teknisiä ja organisatorisia toimenpiteitä, on kyse riskilähtöisyydestä.

mahdollisesti aiheuttamat seuraukset. Tämän pohjalta voidaan päättää hallintakeinoista, joilla haittaan- ja vahingonvaaraan pyritään vaikuttamaan. Riskinhallintakeinot voidaan jakaa niiden luonteen perusteella riskin poistamiseen, siirtämiseen, välttämiseen, mitigoimiseen ja hyväksymiseen.[262]

On kuitenkin syytä huomata, että riskin poistaminen hallintakeinona ei välttämättä poista riskejä kokonaan, sillä se saattaa luoda uusia erilaisia riskejä muun muassa hallintakeinon toimivuuteen liittyen. Riskin poistamisesta tulee erottaa riskin välttäminen, jolla tarkoitetaan tietystä toiminnasta pidättäytymistä kokonaan ja siten riskin täysimääräistä välttämistä.[263] Varsinkin oikeutettuun etuun perustuvassa käsittelyssä riskin välttäminen saattaa olla hyvinkin relevantti riskinhallintakeino, sillä käsittelyn ei tulisi kuitenkaan aiheuttaa kohtuuttoman suurta riskiä yksilön henkilötietojen suojalle. Ennen oikeutettuun etuun perustuvan käsittelyn aloittamista tulisikin laatia erillinen tasapainotesti[264], jossa myös käsittelyn aiheuttamat riskit otetaan huomioon.

Riskienhallinta on kuitenkin vain yksi osa-alue tietoturvan kehitysprosessissa sekä ylläpitämisessä. Riskiperusteisen lähestymistavan painottuminen yleisessä tietosuoja-asetuksessa on johtanut siihen, että tietosuojaviranomaiset ovat julkaisseet paljon riskienhallintaa koskevia käytänteitä.[265] Toisaalta tällaisia käytänteitä on ollut olemassa jo ennen GDPR:n voimaan tulemista, mistä esimerkkinä voidaan mainita sittemmin päivitetty ISO/IEC 27001:2013 -standardi, jota käsittelen jäljempänä. Puolustusministeriön johdolla laadittu kansallinen turvallisuusauditointi kriteeristö (*Katakri 2015*) voi toimia erinomaisena malliesimerkkinä siitä, miten tietosuojaan liittyvää riskienhallintaa tulisi suorittaa. Erityisesti sen turvallisuusjohtamista koskeva kappale on tässä suhteessa olennainen.

Kriteeristöstä löytyy viittauksia myös lainsäädäntöön, joka lisää sen hyödynnettävyyttä muidenkin kuin tietosuojajuridiikan asiantuntijoiden keskuudessa. Vaikka Katakri 2015 on suunnattu nimenomaisesti viranomaisille turvallisuuden kehittämis- ja arviointityökaluna, voi sitä hyödyntää analogisesti myös yksityisellä sektorilla. On huomattava, että GDPR ei aseta julkista sektoria minkäänlaiseen erityisasemaan tietoturva- ja täsmällisyysperiaatteen sovellettavuuden osalta. Kun riskiperusteinen lähestymistapa koskee ainoastaan näitä periaatteita, puoltaa tämä Katakrin analogisen sovellettavuuden mahdollisuutta myös yksityisellä sektorilla. Tämän takia olisi nähtävissä erikoisena

[262] Ks. esim. Andersson 2018, s. 6-7, riskien hallintakeinoista.
[263] VAHTI, 7/2003, s. 21.
[264] Myös Suomen tietosuojavaltuutetun toimiston internetsivuilta löytyy ohjeet tasapainotestin suorittamiseksi: https://tietosuoja.fi/rekisterinpitajan-oikeutettu-etu. Testillä haetaan vastausta ennen kaikkea kysymykseen, *"käykö oikeutettu etu käsittelyn perusteeksi"*.
[265] ICO:n ja tietosuojavaltuutetun toimiston ohjeiden lisäksi esimerkkinä voidaan mainita myös julkisen hallinnon digitaalisen turvallisuuden johtoryhmän VAHTI-ohjeistukset ja kansallinen turvallisuusauditointikriteeristö Katakri 2015, joista ensiksi mainittuun liittyen on tullut päivityksiä GDPR:n myötä. Toisaalta myös Katakri 2015:n laatimisajankohdan aikoihin on ollut varsin selkeä kuva tulevan tietosuoja-asetuksen sisällöstä.

sellainen ratkaisukäytäntö, jossa tietosuojaviranomainen pitäisi Katakrin mukaisia menetelmiä kategorisesti puutteellisina yksityisen sektorin, muttei julkisen sektorin osalta. Toisaalta on syytä todeta, ettei kriteeristö sisällä velvoittavia vaatimuksia, vaan sen tarkoituksena on ainoastaan koota kansallisiin ja kansainvälisiin velvoitteisiin ja vaatimuksiin perustuvia vähimmäisstandardeja sekä esimerkinomaisia tietoturvamenetelmiä.[266]

Katakri 2015:n turvallisuusjohtamista koskevaan osaan T04 sisältyy hyviä käytäntöjä organisaation riskienhallinnan toteuttamiseksi. Koska Katakri 2015:n mukaiset käytännöt on pyritty laatimaan lainsäädännön asettamia velvoitteita vastaaviksi, on perusteltua tuoda niitä esille syvennyttäessä riskienhallintaan oikeusdogmaattisesta näkökulmasta. Katakri 2015:n T04:n mukaan organisaation on

- otettava käyttöön erillinen riskienhallintaprosessi, jossa riskienhallinta on säännöllistä ja jatkuvaa sekä dokumentoitua
- riskien analysoimisessa käytettävä avointa, vakiintunutta ja ymmärrettävää järjestelmällistä menetelmää
- otettava riskienhallinnassa käyttöön säännöllisesti myös organisaation sisäisten tahojen lisäksi ulkopuolisia luotettavia tahoja
- sisällytettävä riskienhallinnan laajuuteen ainakin turvallisuusjohtamisen sekä tila- ja tietoturvallisuuden osa-alueet ja lisäksi näissä tunnistetut riskit on huomioitava tarvittaessa myös sidosryhmien ja toimeksiantosuhteessa olevien osalta
- hyödynnettävä riskienhallintaprosessia ja sen tuloksia organisaation turvallisuustavoitteiden asettamisessa, turvatoimien suunnittelussa, muutoksenhallinnassa, turvallisuuspoikkeamien vaikutusten arvioimisessa ja tarvittaessa myös hankintamenettelyissä
- mitoitettava turvatoimet huomioiden muun muassa tiedon määrä, suojataso, luokitteluperusteet ja sijainnit, mukaan lukien säilytystilat, suhteessa arvioituun rikollisen tai muun vihamielisen toiminnan uhkaan
- dokumentoitava keskeisiltä osin sovellettavat turva- ja valvontatoimet.

Johtopäätöksenä edellä mainitusta voidaan todeta, että organisaation on riskien tunnistamisen lisäksi määriteltävä suojattavat kohteet. Lisäksi niille on nimettävä omistaja ja niihin liittyviin riskeihin on varauduttava riskien tasoon nähden asianmukaisilla suojatoimilla.[267] Riskienhallinnallisten periaatteiden tulee olla selvästi kuvattuja ja niiden on perustuttava järjestelmällisiin prosesseihin. Myös riskienhallinta- ja turvallisuuspäätösten tulee olla dokumentoituja.[268] Näin ollen riskienhal-

[266] Katakri 2015, s. 2—4.
[267] Andersson 2018, s. 4.
[268] Ibid. s. 4.

lintakeinojen sekä tarkemminkin turvallisuustoimien on oltava monimuotoisia eli perustuttava useampien toimenpiteiden yhdistelmään.[269] Koska riskienhallinnan tulee olla avainhenkilöiden ja johdon arvioimaa,[270] on tietosuojakontekstissa syytä nostaa esille myös organisaatiolle mahdollisesti nimitetyn ja sen ylimmälle johdolle raportoivan tietosuojavastaavan keskeinen rooli riskienhallinnassa.

Julkisen hallinnon tiedonhallintaa koskevan lain (*Tiedonhallintalaki*, JTL 906/2019) keskeisenä tavoitteena on asettaa valtionhallinnon viranomaisasiakirjoille luokitteluperusteet ja käsittelyä koskevat tietoturvallisuuteen liittyvät vaatimukset. Tiedonhallintalain 13 §:n mukaan turvallisuustoimenpiteet on mitoitettava suhteessa tietojen merkitykseen sekä tietojärjestelmiin kohdistuviin uhkatekijöihin. JTL:n 12 §:n perusteella viranomaisten toimintaan liittyvät tietoturvallisuusriskit on kartoitettava. Tiedonhallintalain 3.4 § laajentaa edellä mainittua riskienhallintavaatimusta siten, että se voi kohdistua myös yksityisen sektorin toimijoihin, jotka työskentelevät viranomaisten kanssa tai muuten käsittelevät viranomaisten asiakirjoja esimerkiksi konsultin ominaisuudessa. JTL:n 2.1 §:n 9-kohdan sekä 5 §:n mukaan tietoturvallisuustoimet on suunniteltava sekä toteutettava jokaisessa käsittelyvaiheessa ennaltaehkäisevästi. On huomattava, että tiedonhallintalaissa ei ole kuitenkaan kyse pelkästään henkilötietojen suojasta, vaan myös muista syistä salassa pidettäväksi määriteltyjen asiakirjojen tietoturvallisuudesta.

Riskienhallintaan saattaa myös vaikuttaa toimialakohtainen erityissääntely, josta esimerkkinä voidaan mainita teleyrityksiä[271], luottolaitoksia[272], lentoliikennettä[273], energialaitoksia[274] sekä rataverkon haltijoita[275] koskeva erityissääntely. Nähdäkseni tällaisen toimialakohtaisen tietoturvalainsäädännön noudattamisen valvonta kuuluu tietosuojaviranomaisen toimivaltaan siltä osin kuin lainsäädännön tavoitteena on suojata yksilöitä henkilötietojen käsittelyssä, eikä esimerkiksi tiedon luottamuksellisuutta yleiseen tai johonkin muuhun etuun kuin yksilön etuun perustuen. Myös julkisuuslaissa säännellyllä julkisuusperiaatteella on vaikutusta riskienhallinnan kannalta. Toisaalta on huomattava, että julkisuuslaki soveltuu ainoastaan viranomaistoimintaan, mutta yksityisen sektorin toimijoiden, kuten erinäisten konsulttien, on hyvä tuntea kyseinen sääntelyalue viranomaisilta tulleita toimeksiantoja suorittaessaan.

---

[269] Katakri 2015, s. 8—9.
[270] Andersson 2018, s. 4.
[271] Laki sähköisen viestinnän palveluista (917/2014) 282 §.
[272] Laki luottolaitostoiminnasta (610/2014) 9. luku.
[273] EU:n asetus (EY) N:o 216/2008 yhteisistä siviili-ilmailua koskevista säännöistä ja Euroopan lentoturvallisuusviraston perustamisesta sekä neuvoston direktiivin 91/670/ETY, asetuksen (EY) N:o 1592/2002 ja direktiivin 2004/36/EY kumoamisesta (*EASA-asetus*).
[274] Ydinenergialaki (990/1987) 7a §.
[275] Rautatielaki (304/2011) 39 § ja 40 §.

### 4.1.1. Asianmukaiset tekniset ja organisatoriset toimenpiteet

Yleisessä tietosuoja-asetuksessa ja sen johdanto-osassa viitataan asianmukaisiin teknisiin ja organisatorisiin toimenpiteisiin yhteensä 26 kertaa. Tarpeellisten teknisten ja organisatoristen toimenpiteiden vaatimus on siis tullut hyvin keskeiseksi Euroopan tietosuojauudistuksen myötä. Asianmukaisten teknisten ja organisatoristen toimenpiteiden suorittamisen arvioimisen tueksi tarvitaan edellä kuvattua riskienhallintaa. Vain riskien tunnistamisen ja arvioimisen avulla kyetään ennakollisesti osoittamaan teknisten ja organisatoristen toimenpiteiden tarpeellisuus. Näin ollen lopulta valituiksi päätyvien toimenpiteiden on perustuttava organisaation suorittamaan riskien arviointiin. Riskiarvion tulisi ohjata koko organisaatiota henkilötietojen käsittelyssä. Organisaation on sisällytettävä henkilötietojen käsittelyä koskeva riskiarvio osaksi yleisempää riskienhallintaprosessia, jolloin osoitusvelvollisuuden puitteissa on näytettävissä riskilähtöisyyden tulleen huomioiduksi riittävällä tasolla organisaation toiminnassa myös tietosuojan osalta.[276]

Yleisen tietosuoja-asetuksen perusteella tarpeelliset tekniset ja organisatoriset toimenpiteet on liitetty sen riskiperusteisessa ilmenemismuodossa lähtökohtaisesti tietoturvallisuuden[277] ja täsmällisyyden[278] periaatteeseen. Tarpeelliset tekniset ja organisatoriset toimenpiteet mainitaan erikseen myös tietojen minimointiperiaatteen[279] ja säilytyksen rajoittamisen periaatteen[280] yhteydessä sekä osoitusvelvollisuuden täyttämiseen[281] liittyen. Asiakysymysten osalta tekniset ja organisatoriset toimenpiteet on mainittu erikseen pseudonymisoinnin[282], käsittelyn ulkoistamisen[283], sisäänrakennetun ja oletusarvoisen tietosuojan[284], tietoturvaloukkauksesta ilmoittamisen[285], hallinnollisten sakkojen[286] sekä yleisen edun mukaisten arkistointitarkoitusten taikka tieteellisten tai historiallisten tutkimustarkoitusten tai tilastollisten tarkoitusten vuoksi tapahtuvan käsittelyn suojatoimien[287] osalta.

---

[276] VAHTI, 1/2016, s. 21 ja Andersson 2018, s. 6.
[277] GDPR:n 5(1)(f) ja 32(1) artikla, joissa riskiperusteisuus totuttuun tapaan yhdistyy ilmaisuun ”*asianmukaiset tekniset ja organisatoriset toimenpiteet*”.
[278] GDPR:n 5(1)(d) artikla, jossa kylläkin puhutaan kohtuullisista toimenpiteistä, mutta kohtuullisuusarvioinnissa on viranomaisten antamien ohjeistuksien mukaisesti huomioitava nimenomaisesti käsittelyn luonne ja epätäsmällisyyden riski sekä näiden vaikutukset yksilölle.
[279] GDPR:n johdanto-osan 156 kappale sekä 25 ja 89(1) artikla.
[280] GDPR:n 5(1)(e) artikla.
[281] GDPR:n johdanto-osan 78 kappale ja 24(1) artikla.
[282] GDPR:n johdanto-osan 78 kappale ja 4(5) artikla.
[283] GDPR:n johdanto-osan 81 kappale ja 28 artikla.
[284] GDPR:n 25 artikla, jossa asianmukaiset tekniset ja organisatoriset toimenpiteet liitetään laajemmin kaikkien tietosuojaperiaatteiden täytäntöönpanoon, mutta GDPR:ssä omaksuttuun tapaan tällöin riskiperusteisuus ei yhdisty kyseiseen ilmaisuun.
[285] GDPR:n 34(3)(a) artikla, jossa asianmukaiset tekniset ja organisatoriset toimenpiteet pohjimmiltaan liitetään suojatoimiin ja erityisesti pseudonymisoimiseen.
[286] GDPR:n 83(2)(d) artikla.
[287] GDPR:n 89(1) artikla.

Yhteenvetona voidaan todeta, että tietojenkäsittelyssä on asianmukaisin teknisin ja organisatorisin toimenpitein huolehdittava kaikkien tietosuojaperiaatteiden noudattamisesta. Toimien asianmukaisuutta tulee arvioida riskilähtöisesti puolestaan tietotuvallisuuden ja täsmällisyyden periaatteiden osalta. Muilta osin kyse on puhtaasti lainsäädäntöön perustuvasta toimenpiteiden tarpeellisuuden harkinnasta, etenkin osoitusvelvollisuuden, tietojen minimoinnin, säilytyksen rajoittamisen ja sisäänrakennetun sekä oletusarvoisen tietosuojan täyttämiseksi. Lisäksi rekisterinpitäjän vastuuta koskevan tietosuoja-asetuksen 24(1) artiklan mukaan teknisten ja organisatoristen toimenpiteiden tarpeellisuutta on tarkistettava ja päivitettävä tarvittaessa.

### 4.1.2. Ennakkovalvonta

Ennakkovalvonnassa on kyse haittojen ja vahinkojen ennaltaehkäisystä, pyrkimällä viranomaisjohtoisesti vähentämään toiminnasta aiheutuvia riskejä tai jopa estämään suhteettoman riskialttiin toiminnan aloittaminen. Tyypillisesti ennakkovalvontaa on käytetty kontrollikeinona sellaisessa toiminnassa, josta aiheutuva haitta tai vahinko voidaan nähdä hyvin merkittävänä ja tällaisten vahinkojen kompensoiminen haastavana. Ennakkovalvontaa on totuttu näkemään erityisesti ympäristöoikeuden alueella muun muassa ympäristövaikutusten ennakkoarvioinnin muodossa.[288] Suomessa ennakkovalvontaa suorittavia viranomaisia ovat olleet aluehallintovirastot (AVI) ja Elinkeino-, liikenne- ja ympäristökeskukset (ELY-keskus), joiden toiminnasta on kertynyt hyvää hallintoa ennakkovalvonnassa koskevaa oikeuskäytäntöä. Sitä voidaan analogisesti hyödyntää otettaessa kantaa tietosuojaviranomaisen ennakkovalvonnassa soveltamaan hyvän hallinnon periaatteeseen.[289]

Yleisen tietosuoja-asetuksen puitteissa ennakkovalvontaa koskeva sääntely keskittyy tietosuoja-asetuksen 36 artiklan mukaiseen tietosuojaviranomaisen ennakkokuulemiseen ja 35 artiklan mukaiseen tietosuojaa koskevaan vaikutustenarviointiin. Vaikutustenarvioinnissa ei vielä kuitenkaan ole kyse varsinaisesti viranomaisen ennakkovalvonnasta. Ennakollisesta viranomaisvalvonnasta on kyse vasta ennakkokuulemisessa, johon ryhdytään, mikäli sen edellytykset katsotaan vaikutustenarvioinnin pohjalta täyttyviksi.

Vaikutustenarvioinnin suorittaminen edellyttää kuitenkin rekisterinpitäjän mahdollisesti GDPR:n 37 artiklan nojalla nimittämän tietosuojavastaavan kuulemista. Jonkin asteista neutraalilla tavalla ennaltaehkäisevää vaikutusta pitäisi kuitenkin olla myös tietosuojavastaavan kuulemisellakin, sillä GDPR:n 38(3) artiklan mukaisesti tietosuojavastaavan tulee toimia tehtävässään riippumattomasti, eikä rekisterinpitäjä tai henkilötietojen käsittelijä saa erottaa tai rangaista tietosuojavastaavaa sen vuoksi, että tämä on hoitanut tehtäviään. Samassa säännöksessä todetaan tietosuojavastaavan rapor-

[288] Ks. esim. Hollo 2010, s. 4, viranomaisen suorittaman ennakkovalvonnan perusteista.
[289] Belinskij et al. 2016, s. 21.

toivan tehtävissään havaitsemistaan seikoista suoraan rekisterinpitäjän tai henkilötietojen käsittelijän ylimmälle johdolle. Tietosuojavastaava ei ole kuitenkaan viranomaistaho, eikä se näin ollen suorita tehtäväänsä virkavastuulla.

Tiivistäen, mikäli henkilötietojen käsittelyyn kohdistuu erityisen korkea riski, on rekisterinpitäjän tällöin laadittava tietosuojaa koskeva *vaikutustenarviointi*, josta säädetään tietosuoja-asetuksen 35 artiklassa sekä johdanto-osan 84, 89—93 sekä 95 kappaleissa. Vaikutustenarviointi tulisi tehdä erityisesti silloin, kun käyttöönotetaan uutta teknologiaa[290], joka on tyypillistä esimerkiksi henkilötietojen käsittelyä ulkoistettaessa. Kun käsittelyn tarkoituksen perusteella on havaittavissa henkilötietojen käsittelyn kohdistuvan suureen määrään henkilötietoja tai käsittelytoimet vaikuttavat suureen määrään rekisteröityjä, tulisi vaikutustenarviointi myös näissä tilanteissa suorittaa.[291]

On syytä huomata, että vaikutustenarvioinnin suorittaminen ei edellytä korkeaa riskitasoa ja vaikutustenarvioinnin voikin toteuttaa myös matalariskisten toimenpiteiden yhteydessä. Edellä mainittua voidaankin pitää suositeltavana, sillä näin rekisterinpitäjän velvollisuudet tulevat selvitetyiksi. Tästä on apua myös ulkoistustilanteissa, kun laaditaan tietojenkäsittelysopimusta, jossa joka tapauksessa tulee määritellä rekisterinpitäjän sekä henkilötietojen käsittelijän tietosuojavelvoitteet.[292]

Vaikutustenarvioinnissa suunniteltaville toimenpiteille määritellään asianmukainen suojataso ja tarkastellaan täyttävätkö suunnitellut suojatoimet ja mekanismit asianmukaiseksi arvioidun tietoturvan tason. Vaikutusarvioinnin ei tule jäädä merkityksettömäksi toimenpiteeksi, vaan rekisterinpitäjän tulee vaikutustenarvioinnin jälkeen varmistaa, että henkilötietoja käsitellään vaikutustenarvioinnin mukaisesti myös käytännössä. Mikäli vaikutustenarvioinnin perusteella rekisterinpitäjä ei ryhdy toimenpiteisiin riskin pienentämiseksi, on sen tällöin toimitettava valvontaviranomaiselle perustiedot käsittelytoimista ja kuultava valvontaviranomaista preventiivisesti, ennen käsittelytoimien aloittamista.

Edellä mainitulla *ennakkokuulemisvelvoitteella* tarkoitetaan tietosuoja-asetuksen 35 artiklan mukaisesti riskiperusteista ilmoitusvelvollisuutta.[293] Kyse ei siis enää ole henkilötietolain mukaisesta yleisestä ilmoitusvelvollisuudesta, joka kytkeytyi oikeutetun edun puitteissa tapahtuneeseen käsittelyyn. Vaikutustenarvioinnin laatimisvelvollisuuteen johtavista käsittelytyypeistä voidaan kansallisen tietosuojaviranomaisen puolesta, tai vastaavasti rajat ylittävässä käsittelyssä, tietosuojaneuvoston toimesta, julkaista luettelo, jonka sisällöstä rekisterinpitäjän tulee olla tietoinen.[294]

---

[290] GDPR:n johdanto-osan 89 kappale.
[291] Oikeusministeriön selvityksiä ja ohjeita, 4/2017, s. 17.
[292] Ibid. s. 18.
[293] Tietosuojavaltuutetun toimiston tiedote, 1.3.2018, tietosuojavaltuutetun uusista tehtävistä.
[294] Oikeusministeriön selvityksiä ja ohjeita, 4/2017, s. 18.
Ks. ennakkokuulemismenettelystä myös GDPR:n johdanto-osan 94—96 kappaleet.

#### 4.1.2.1. Vaikutustenarviointi

Yleisen tietosuoja-asetuksen riskiperusteinen lähestymistapa ilmenee muun ohella organisaation riskienarviointivelvollisuutena, johon viittaa asetuksen 35 artiklan määrittelemä tietosuojaa koskeva vaikutustenarviointi (DPIA, engl. *Data Protection Impact Assessment*). Tämä ei kuitenkaan tarkoita sitä, että rekisterinpitäjä tai henkilötietojen käsittelijä olisi vapautettu riskienarviointivelvoitteesta muissa kuin vaikutustenarvioinnin soveltamisalaan kuuluvissa tilanteissa. Kuten edellä on todettu, kyseinen velvoite kuuluu olennaisena osana täsmällisyyden ja tietoturvallisuuden periaatteiden soveltamiseen, joiden noudattamista edellytetään sekä rekisterinpitäjältä että henkilötietojen käsittelijältä kaikissa käsittelytilanteissa.

Tietosuoja-asetuksen 35(1) artiklan mukaan DPIA tulee laatia aina, kun henkilötietojen käsittely todennäköisesti aiheuttaa luonnollisen henkilön oikeuksille ja vapauksille korkean riskin. Arvioinnissa on otettava huomioon käsittelyn luonne, asiayhteys, laajuus sekä tarkoitukset. Säännöksen mukaan etenkin uuden teknologian käyttöönottamisen yhteydessä tarve vaikutustenarvioinnille voi olla olemassa. Kuten todettu, rekisterinpitäjän on pyydettävä tietosuojavastaavaltaan neuvoa DPIA:ta varten, mikäli tietosuojavastaava on nimetty.[295] Tilanteessa, jossa organisaation ei kokonsa puolesta tarvitse nimetä tietosuojavastaavaa olettamana todennäköisesti on se, että tällaisten tilanteiden arvioimiseen osallistuu yhtiön korkein johto, sillä tietosuojavastaavan tehtäviin kuuluu raportoida toiminnastaan yhtiön ylimmälle johdolle.[296]

Tietosuoja-asetuksen 35(3) artikla sisältää esimerkinomaisen luettelon tilanteista, joissa vaikutustenarviointi vaaditaan. Säännöksen mukaan DPIA tulee laatia

- järjestelmällisen ja kattavan tietosuoja-asetuksen tarkoittaman profiloinnin ja automatisoidun päätöksenteon yhteydessä[297]
- laajamittaisen käsittelyn yhteydessä, jos se kohdistuu henkilötietojen erityisryhmiin[298] taikka rikostuomioita ja rikkomuksia[299] koskeviin tietoihin
- yleisölle avoimen alueen järjestelmällisen ja laajamittaisen valvonnan käsillä ollessa[300].

On syytä huomata, että listauksen esimerkinomaisuudesta huolimatta se on sanamuodon mukaisesti ehdoton. Toisin sanoen ainakin listassa mainituissa tilanteissa vaikutustenarviointi on laadittava. Muissa kuin erikseen listatuissa tapauksissa DPIA:n tarpeellisuutta tulee arvioida asetuksen 35(1)

---

[295] GDPR:n 35(2) artikla.
[296] Ks. esim. Andersson 2018, s. 6.
[297] Tutkielman III osan kappaleessa 4.1.3. käsitellään sitä, milloin kyse on GDPR:n mukaisesta profiloinnista tai automatisoidusta päätöksenteosta.
[298] Tutkielman III osan kappaleessa 4.1.5. käsitellään henkilötietojen erityisryhmiin kuuluvien tietojen käsittelyä.
[299] Tutkielman III osan kappaleessa 4.1.3. käsitellään rikostuomioita ja rikkomuksia koskevien tietojen käsittelyä.
[300] Tässä kohdassa viitataan julkisessa tilassa tapahtuvaan tallentavaan kameravalvontaan.

artiklan mukaisesti, jolloin uuden teknologian käyttöönottaminen on käsittelyn luonteen, laajuuden, asiayhteyden ja tarkoituksen ohella avainkriteerinä arvioitaessa yksilön oikeuksille ja vapauksille muodostuvan korkean riskin todennäköisyyttä. Esimerkiksi uuden teknologian käyttöönottaminen sellaisen henkilötietojen erityisryhmiin kuuluvien tietojen käsittelyn osalta, mikä ei ole kuitenkaan edellä mainitun edellytyksen mukaisesti laajamittaista, voinee puoltaa vaikutustenarvioinnin tarpeellisuutta.[301]

Vaikutustenarvioinnin kohteena voi olla joko yksittäinen käsittelytoimi taikka useampia samankaltaisia käsittelyprosesseja.[302] Asetuksen 35(7) artiklan mukaan arvioinnin tulee sisältää ainakin

- käsittelytoimien kuvauksen, tarkoituksen sekä rekisterinpitäjän oikeutetun edun[303], mikäli se on käsittelyn oikeusperusteena
- arvion käsittelytoimien oikeasuhteisuudesta ja tarpeellisuudesta käsittelyn edellä mainittuihin tarkoituksiin nähden
- arvion rekisteröityjen oikeuksille ja vapauksille kohdistuvasta riskistä[304]
- suunnitelman toimenpiteistä riskeihin vaikuttamiseksi, pitäen sisällään turvallisuus- ja suojatoimet sekä mekanismit, joilla varmistetaan henkilötietojen suoja ja osoitetaan, että tietosuoja-asetusta noudatetaan huomioiden rekisteröityjen ja muiden asianomaisten oikeudet ja oikeutetut edut.

Näin ollen vaikutustenarvioinnissa on kyse riskienhallintaan kuuluvasta riskien tunnistamisesta ja arvioimisesta sekä toisena elementtinä riskienhallintaan kuuluvasta riskienhallintakeinojen valitsemisesta eli riskeihin puuttumisesta. Keinojen on oltava oikeassa suhteessa arvioituihin riskeihin nähden. Lisäksi käsittelytoimien tarpeellisuutta on erikseen arvioitava, jolla viitataan erityisesti riskien välttämisen riskienhallintakeinoon. Toisaalta riskien arvioinnissa tulee määritellä myös käsittelyn tarkoitus ja kuvaus, mutta käytännössä nämä toimenpiteet tulee suorittaa kaikkien henkilötietojen käsittelyprosessien osalta. Lisäksi käsittelyperuste tulee aina määritellä, jolloin oikeutetun edunkin tulisi olla tasapainotestin puitteissa tiedossa myös silloin, kun riskienarvioinnille ei ole tarvetta.

Mikäli riskeissä tapahtuu muutoksia, on rekisterinpitäjän arvioitava, onko DPIA aihetta laatia tai jo aikaisemmin laadittua DPIA:ta aihetta muuttaa.[305] Vaikutustenarviointi on erityisen tärkeä työkalu

---

[301] Huomaa, että myös jäljempänä esitetyn oletusarvoisen ja sisäänrakennetun tietosuojan vaatimus edellyttää näissä tapauksissa jo jonkin asteista riskianalyysiä (Privacy by Design). Ks. tutkielman III osan kappale 4.2. sisäänrakennetusta ja oletusarvoisesta tietosuojasta.
[302] GDPR:n 35(1) artikla.
[303] Näin ollen DPIA:han tulisi sisällyttää tasapainotesti (*Legitimaten interest assessment*).
[304] Vain jos riski on korkea, tulee ryhtyä ennakkokuulemiseen. Vaikutustenarviointi puolestaan suoritetaan, mikäli käsittely aiheuttaa todennäköisesti, muttei välttämättä, korkean riskin.
[305] Andersson 2018, s. 7.

nimenomaan rekisterinpitäjän osoitusvelvollisuuden täyttämiseksi.[306] DPIA:n funktiona on auttaa rekisterinpitäjää noudattamaan tietosuoja-asetusta sekä osoittamaan, että asetuksen mukaisia tietosuojaperiaatteita noudatetaan.[307] Näin ollen vaikutustenarvioinnin tarpeellinen sisältö määräytyy tosiasiassa aikaisemmin kuvattujen tietosuojaperiaatteiden kautta, DPIA:lle määriteltyjen muotomääräysten lisäksi.

Tietosuoja-asetuksen 35(9) artiklan mukaan rekisterinpitäjän on tapauskohtaisesti pyydettävä rekisteröityjen taikka näiden edustajien näkemyksiä suunnitelluista käsittelytoimista ilman, että se vaikuttaa yleisten etujen suojeluun, käsittelytoimien turvallisuuteen tai kaupallisesti. Tällaisen käsittelyn kohdistuessa esimerkiksi rekisterinpitäjän työntekijöihin voidaan käsittelytoimien läpikäymistä yhteistoimintamenettelyn yhteydessä työntekijöiden edustajien kanssa pitää aiheellisena. Yhteistoimintaa yrityksissä koskevan lain (Yhteistoimintalaki, 334/2007) mukaan monet henkilötietojen käsittelyä koskevat ohjeet voidaan sisällyttää yhteistoimintamenettelyn piiriin. Lisäksi kameravalvonnan käyttöönoton ja kulunvalvonnan sekä työsähköpostin ja tietoverkon käytön periaatteiden kuten myös yksityisyydensuojasta työelämässä annetun lain (YksTL, 756/2004) 7 ja 8 §:ssä tarkoitetun huumausainetestitulosten käsittelemisen työnantajan toimesta edellytetään kuuluvan YksTL:n sekä yhteistoimintalain 19.1 §:n mukaan yhteistoimintamenettelyn piiriin.[308] Näissä kaikissa toiminnoissa on kyse henkilötietojen käsittelystä.

Mikäli henkilötietoja käsitellään rekisterinpitäjän *lakisääteisen velvoitteen* nojalla taikka jos *oikeutettuun etuun* perustuvan käsittelyn taustalla on rekisterinpitäjään sovellettava unionin oikeus tai jäsenvaltion lainsäädäntö, voidaan tietosuoja-asetuksen 35(1)—(7) artikloja olla soveltamatta. Tällöin unionin tai jäsenvaltion lainsäädännössä tulee säännellä käsittelytoiminnasta siten, että tietosuojaa koskeva vaikutustenarviointi on jo tehty yleisen vaikutustenarvioinnin osana kyseisen oikeusperusteen hyväksymisen yhteydessä, ellei jäsenvaltio katso DPIA:n laatimista tarpeelliseksi ennen käsittelytoimien aloittamista.[309] Edellä mainitulla yleisellä vaikutustenarvioinnilla tarkoitetaan sitä vaikutustenarviointia, joka sisältyy käsittelytoimien aloittamiseen myös silloin, kun tietosuoja-asetuksen 35 artiklan mukaisen DPIA:n edellytyksenä oleva todennäköinen rekisteröityjen oikeuksiin ja vapauksiin kohdistuva korkea riski ei olisikaan käsillä. Tällöin erillinen asetuksen 35 artiklassa tarkoitettu vaikutustenarviointi on laadittava ainoastaan, mikäli laissa sitä erikseen edellytetään.

---

[306] Tietosuojatyöryhmän ohje, WP 248, s. 4, korkean riskin määrittelystä.
[307] Ibid. s. 4.
[308] Vastaavan sisältöiset vaatimukset on säädetty yhteistoiminnasta valtion virastoissa ja laitoksissa annetun lain (1233/2013) 13.1 §:ssä. On huomattava, että työnantajan ja henkilöstön välisestä yhteistoiminnasta kunnissa annetussa laissa (449/2007) vastaavan laajuisia, yksityiskohtaisia yhteistoimintavelvoitteita ei ole säädetty, mikä voidaan nähdä ongelmallisena tietosuojan kannalta ja erityisesti DPIA:ta koskevan artiklan yhdenmukaisuuden näkökulmasta. Tällöin kunnallinen työnantaja ei voi käytännössä soveltaa GDPR:n 35(10) artiklan mukaista poikkeussääntöä tai ainakin työntekijöiden kuuleminen on jollakin erityisellä tavalla järjestettävä.
[309] GDPR:n 35(10) artikla.

Edellä mainitusta johtuen rekisterinpitäjän käsitellessä esimerkiksi henkilötietojen erityisryhmiin kuuluvia työntekijöiden lääkärintodistuksia[310] lakisääteisiin velvoitteisiinsa perustuen, ja vaikka tällaisessa tilanteessa oltaisiin otettu käyttöön uutta teknologiaa, ei vaikutustenarviointia tarvitse laatia. Edellä mainittu poikkeaminen GDPR:n 35 artiklasta on mahdollista todennäköisen korkean riskin käsillä ollessa, ellei lainsäädännöstä erikseen muuta johdu. On kuitenkin huomattava, että mainittu poikkeus ei poista todennäköisen korkean riskin käsillä ollessa velvollisuutta tapauksen mukaan pyytää rekisteröityjen tai näiden edustajien näkemyksiä suunnitelluista käsittelytoimista, mistä toisaalta saatetaan työsuhteen kontekstissa säännellä jo yhteistoimintalaissakin.

Mikäli rekisterinpitäjä tai henkilötietojen käsittelijä noudattaa käsittelyssä hyväksyttyjä käytännesääntöjä, on ne relevanttia ottaa huomioon arvioitaessa näiden käsittelytoimien vaikutusta erityisesti tietosuojaa koskevassa vaikutustenarvioinnissa.[311] Vaikka säännöksessä ei sitä erikseen mainita, on selvää, että myös sertifiointimekanismien käyttämisellä on vaikutusta DPIA-menettelyyn. Käsittelen tietosuoja-asetuksen 40 artiklan mukaisia hyväksyttyjä käytännesääntöjä ja 42 artiklan mukaisia sertifiointimekanismeja jäljempänä tutkielman III osan kappaleessa 4.4.

Tietosuoja-asetuksen 35(5) artiklan mukaan tietosuojaviranomaisen on mahdollista laatia ja julkaista luetteloita tilanteista, joissa ei ainakaan tarvitse suorittaa vaikutustenarviointia. Vastaavasti tietosuojaviranomainen voi asetuksen 35(4) artiklan nojalla julkaista listan tilanteista, joissa vaikutustenarviointi tulee laatia. Toisaalta tavaroiden tai palveluiden myynnin tai niiden seurannan kohdistuessa useampaan jäsenvaltioon samanaikaisesti taikka jos toimet voivat merkittävästi vaikuttaa henkilötietojen vapaaseen liikkuvuuteen unionin alueella, on toimivaltaisen tietosuojaviranomaisen sovellettava poikkeuksellisesti tietosuoja-asetuksen 63 artiklan mukaista yhdenmukaisuusmekanismia ennen luettelon vahvistamista.[312] Muussa tapauksessa edellä mainitut luettelot tulevat vahvistetuiksi toimivaltaisen kansallisen tietosuojaviranomaisen toimitettua ne unionin tietosuojaneuvostolle.[313]

#### 4.1.2.2. Ennakkokuuleminen

Ennakkokuulemiseen on ryhdyttävä, mikäli edellä kuvatun vaikutustenarvioimisen pohjalta päädytään siihen, että rekisteröidyn oikeuksiin ja vapauksiin kohdistuvan todennäköisen korkean riskin sijaan käsittely aiheuttaa todellisen korkean riskin, eikä rekisterinpitäjä ole kyennyt toteuttamaan sellaisia toimenpiteitä, joilla riski pienenisi riittävästi.[314] Tietosuoja-asetuksen 35(2) artiklan mu-

[310] Käsittely perustuu varhaiseen puuttumiseen ja sairauspäivärahahakemusten käsittelyyn (HE 75/2011 vp, s. 14).
[311] GDPR:n 35(8) artikla.
[312] GDPR:n 35(6) artikla.
[313] GDPR:n 35(4) ja (5) artikla.
[314] GDPR:n 36(1) artikla.

kaan tietosuojaviranomainen voi asetuksen mukaisia valtuuksiaan käyttäen, kahdeksan viikon kuluessa kuulemispyynnöstä, antaa rekisterinpitäjälle ohjeet tietosuoja-asetuksen noudattamiseksi, jotta korkean riskin rekisteröidylle aiheuttavassa käsittelyssä noudatettaisiin sovellettavaa tietosuojalainsäädäntöä. Suunnitellun käsittelyn monimutkaisuuden perusteella määräaikaa voidaan jatkaa enintään kuudella viikolla.

Näin ollen lähtökohtana on ennakkovalvonnalle tyypilliseen tapaan, että suunniteltuja toimenpiteitä ei aloiteta ennen kuin viranomainen on hyväksynyt käsittelyn aloittamisen taikka antanut tarkemmat ohjeet käsittelyn aloittamiseksi. On kuitenkin huomattava, että valvontaviranomainen voi jatkaa määräaikaa vielä kuuden viikon määräajanpidennyksen jälkeenkin, mikäli tämä ei ole saanut tarvittavia tietoja rekisterinpitäjältä tai henkilötietojen käsittelijältä käsittelyyn liittyen. Kyseinen määräajanpidennys ei saa johtua viranomaisen vastuulla olevista syistä.

Rekisterinpitäjän on tietosuoja-asetuksen 26(3) artiklan mukaan toimitettava valvontaviranomaiselle ennen tämän kuulemista

- tarvittaessa rekisterinpitäjän, yhteisrekisterinpitäjien ja käsittelyyn osallistuvien henkilötietojen käsittelijöiden vastuualueet erityisesti konsernin sisällä suoritettavaa käsittelyä varten
- suunnitellun käsittelyn keinot[315] ja tarkoitus
- tietoturvatoimenpiteet rekisteröityjen oikeuksien ja vapauksien suojaamiseksi
- tietosuojavastaavan yhteystiedot, mikäli sellainen on nimetty organisaatiolle
- vaikutustenarviointi
- muut valvontaviranomaisen erikseen pyytämät tiedot.

Käytännössä kuulemismenettelyssä toimitettavat tiedot poikkeavat vaikutustenarvioinnin vaaditusta sisällöstä siltä osin, että eri organisaatioiden vastuualueet on listattava ja tietosuojavastaavan yhteystiedot on toimitettava. Lisäksi valvontaviranomainen voi tapauksen mukaan pyytää muita erityisiä tietoja käsittelyyn liittyen. Vastuualueiden määrittäminen on tarpeellista, jotta viranomainen kykenee kohdistamaan edellyttämiään toimenpiteitä oikeille tahoille.[316]

Yleisen tietosuoja-asetuksen 36(4) artiklassa säädetään vielä erityisestä kuulemismenettelystä, joka sitoo lainsäädäntöprosesseissa. Tietosuojaviranomaista on kuultava lainsäädäntötoimenpiteiden valmistelussa, mikäli lainsäädännöllä on vaikutusta henkilötietojen käsittelyyn. Lisäksi tietosuoja-

[315] Tämä pitää sisällään muun muassa mahdollisesti hyödynnettävät automatisoidun päätöksenteon taikka profiloinnin menetelmät.

[316] Vastuualueita ei mainita DPIA:n osalta todennäköisesti siksi, että näiden tietojen oletetaan olevan ilman erillistä selvitystäkin rekisterinpitäjän tiedossa, mutta ulkopuolinen tarkastelija ei niitä voi välttämättä havaita. On selvä asia, että myös DPIA:n yhteydessä ja laajemminkin kaiken riskilähtöisen lähestymistavan osalta vastuualueilla on merkittävä rooli asianmukaisten toimenpiteiden toteuttamisessa.

asetuksen 36(5) artiklan mukaan jäsenvaltio voi kansallisessa lainsäädännössään edellyttää ennakkokuulemista yleiseen etuun perustuvan käsittelyn suorittamiseksi, mukaan lukien käsittelyyn kansanterveyden ja sosiaaliturvan alalla liittyen. Vielä henkilötietodirektiivin voimassaollessa sosiaalisiin etuuksiin liittyvät henkilötiedot oli määritelty arkaluonteisiksi. Vaikka nykyään näin ei enää ole, kuulemismenettelyä koskevassa säännöksessä nimenomaisesti painotetaan, että kyseisissä tapauksissa erityisen kuulemisvelvoitteen säätäminen kansallisessa lainsäädännössä voi olla perusteltua.

Yhteenvetona voidaan todeta, että ennakkokuulemiseen tulee ryhtyä ainoastaan, mikäli DPIA:n pohjalta on todettavissa, että henkilötietojen käsittelyprosessista muodostuu korkea jäännösriski rekisteröidylle. Vaikutustenarviointia koskeva säännös nimittäin edellyttää, että rekisterinpitäjän tulee riskinhallintakeinojen avulla vähentää riskiä, mikäli se on mahdollista. Jos riski jää tästä huolimatta korkeaksi, tulee ryhtyä ennakkokuulemiseen. Peruslähtökohtana on siis se, ettei korkean riskin rekisteröidyille aiheuttaviin käsittelytoimiin tulisi ryhtyä. Jos rekisterinpitäjä ei kykene itse määrittämään riittäviä tietosuojatoimia riskin pienentämiseksi, on vielä mahdollista, että viranomaiselta löytyy tähän riittävät työkalut ja menetelmät.[317] Vaikutusarvioinnin sekä ennakkokuulemisen tarkoituksena on siis löytää riittävät riskienhallintakeinot käsittelytoimien aiheuttamaan korkeaan riskiin puuttumiseksi.

### 4.1.3. Automatisoitu päätöksenteko ja profilointi

Yleisen tietosuoja-asetuksen 4(4) artiklan mukaan profiloinnilla tarkoitetaan mitä tahansa henkilötietojen automatisoitua käsittelyä, jossa henkilötietoja käyttämällä arvioidaan yksilön tiettyjä henkilökohtaisia ominaisuuksia[318]. Profilointi voi olla automaattista tai osittain automaattista, mutta sen tulee joka tapauksessa kohdistua henkilötietoihin, ja henkilökohtaisten ominaisuuksien arvioimisen tulee olla sen tarkoituksena, jotta kyse voisi olla tietosuoja-asetuksessa tarkoitetusta profiloinnista.[319]

Automaattinen päätöksenteko ei ole puolestaan saanut omaa määritelmää tietosuoja-asetuksen 4 artiklaan. Automatisoidut päätöksentekotilanteet voidaan jakaa tietosuojalainsäädännön näkökulmasta tilanteisiin, joissa on kyse pelkästään automaattiseen henkilötietojen käsittelyyn perustuvasta päätöksenteosta sekä tilanteisiin, joissa päätöksillä on oikeusvaikutuksia tai tällaiset päätökset muuten vaikuttavat rekisteröityyn merkittävästi.[320] Vain jälkimmäisessä tapauksessa automatisoitua

[317] Tietosuojatyöryhmän ohje, WP 248, s. 7.
[318] GDPR:n 4(4) artiklan mukaan profiloinnista on kyse erityisesti silloin, kun automatisoidusti *"analysoidaan tai ennakoidaan piirteitä, jotka liittyvät kyseisen luonnollisen henkilön työsuoritukseen, taloudelliseen tilanteeseen, terveyteen, henkilökohtaisiin mieltymyksiin, kiinnostuksen kohteisiin, luotettavuuteen, käyttäytymiseen, sijaintiin tai liikkeisiin"*.
[319] Tietosuojavaltuutetun toimiston ohje: Automaattinen päätöksenteko ja profilointi.
[320] Ibid.

päätöksentekoa koskeva seuraavaksi kuvattu lähtökohtainen kielto on sovellettavissa. Kuvaan automaattisen päätöksenteon, profiloinnin ja henkilötietojen erityisryhmiin sekä rikoksiin ja rikkomuksiin kuuluvien tietojen käsittelyn erikseen omissa kappaleissa, sillä näiden osalta on kyse riskilähtöisyyden kannalta tietosuoja-asetuksessa säännellyistä erityistilanteista.

On huomattava, että päätöksiä voidaan tehdä automaattisesti ilman profilointia ja toisaalta profilointia voidaan suorittaa ilman automaattista päätöksentekoa. Lisäksi samaan käsittelyprosessiin voi sisältyä molemmat elementit yhtäaikaisesti. Profiloinnin avulla luotu henkilörekisteri voi olla automatisoidun päätöksenteon pohja-aineistona. Tietosuojavaltuutetun toimiston antamissa ohjeissa todetaankin, että automaattinen päätöksenteko voi perustua rekisteröidyltä saatuun tietoon, havaintojen avulla kerättyihin tietoihin sekä pääteltyyn tai tietyistä tiedoista johdettuun tietoon. Vain jälkimmäisessä tietystä aineistosta johdetussa tietojen käsittelyssä on kyse automatisoituun päätöksentekoon sisältyvästä profilointielementin.[321]

Aina kun rekisterinpitäjä ryhtyy automatisoituun päätöksentekoon, on rekisteröidylle ilmoitettava käsittelystä ja annettava mahdollisuus vaatia luonnollisen henkilön osallistumista päätöksentekoon sekä ilmoitettava tarkemmin, mitä tietoja käsitellään ja mikä on päätöksentekoprosessin logiikka.[322] Informoinnissa on otettava huomioon selkeyden ja yksinkertaisen kielen vaatimus. Tällöin informoinnin sisältöä tulisi tarkastella erityisesti rekisteröidylle mahdollisesti käsittelystä aiheutuvien seurausten ja niiden merkittävyyden näkökulmasta[323]. Myös algoritmeja on tarkastettava säännöllisesti, kuten muitakin riskianalyysiin vaikuttavia seikkoja.[324]

Tietosuoja-asetuksen 22(1) artiklan mukaan ”*rekisteröidyllä on oikeus olla joutumatta sellaisen päätöksen kohteeksi, joka perustuu pelkästään automaattiseen käsittelyyn, kuten profilointiin, ja jolla on häntä koskevia oikeusvaikutuksia tai joka vaikuttaa häneen vastaavalla tavalla merkittävästi”*. Jo henkilötietodirektiivin voimassa ollessa automatisoitua päätöksentekoa koski vastaavanlainen oikeus olla joutumatta tällaisen käsittelyn kohteeksi. Nykyinen tietosuojalainsäädäntö asettaa samat vaatimukset myös profilointiin liittyen.

Asetuksen 22(2) artiklan mukaisen poikkeussäännöksen nojalla lähtökohtaista kieltoa ei noudateta, mikäli käsittely on välttämätöntä rekisteröidyn ja rekisterinpitäjän välisen *sopimuksen*[325] täytäntöön

---

[321] Tietosuojavaltuutetun toimiston ohje: Automaattinen päätöksenteko ja profilointi.
[322] Ibid.
[323] Ibid. Informoinnissa voisikin kiinnittää huomiota erityisesti siihen, miksi tietoja käsitellään, mitä päätöksenteossa painotetaan sekä eri tietojen painoarvot ja mikä on tietojen alkuperä, miten oikeudenmukaisuus varmistetaan jatkuvasti, yhteystiedot päätöksen uudelleen arvioimista varten, käsittelyn vaikutukset rekisteröityyn ja tiedot suunnitelluista tulevista toimenpiteistä.
[324] Linder 2016, s. 39—40.
[325] Tietosuojavaltuutetun toimiston ohjeiden mukaan kyse voi olla esimerkiksi rahoitussopimuksesta ja siihen liittyvästä automatisoidusta luottoluokittelusta (profilointi) tai luottokelpoisuuden määrittämisestä yksittäistapauksessa (automatisoitu päätöksenteko).

panemiseksi, *sovellettavan lainsäädännön* nojalla edellyttäen, että tällaisessa lainsäädännössä vahvistetaan asianmukaiset toimenpiteet rekisteröityjen oikeuksien ja vapauksien sekä muiden oikeutettujen etujen suojaamiseksi taikka käsittelyn perustuessa nimenomaiseen asianomaisen rekisteröidyn antamaan *suostumukseen*. On huomattava, että jokaisen oikeus olla joutumatta automaattisen päätöksenteon kohteeksi on liitettävissä myös oikeutettuun etuun perustuvassa käsittelyssä sovellettavaan rekisteröidyn oikeuteen vastustaa henkilötietojen käsittelyä.[326]

Tietosuoja-asetuksen 22(3) artiklan mukaan rekisterinpitäjän on toteutettava asianmukaiset toimenpiteet rekisteröidyn oikeuksien ja vapauksien sekä oikeutettujen etujen suojaamiseksi, mikäli profilointi tai automatisoitu päätöksenteko perustuu rekisteröidyn suostumukseen tai sopimuksen tekemiseen taikka sen täytäntöönpanemiseen. Tällöin rekisteröidylle on annettava mahdollisuus erikseen vaatia luonnollisen henkilön osallistumista käsittelyyn sekä oikeus esittää kantansa ja tarvittaessa riitauttaa päätös. Tässä yhteydessä päätöksellä ei viitata ainoastaan automatisoidun päätöksenteon myötä syntyneeseen yksilön oikeuksiin ja vapauksiin kohdistuvaan päätökseen, vaan myös profiloinnin suorittamiseksi syntyneeseen päätökseen sisällyttää rekisteröity tiettyyn ryhmään. Tällaisella päätöksellä voi olla tosiasiallista vaikutusta rekisteröidyn oikeudelliseen asemaan tulevaisuudessa.

Tietosuoja-asetuksen 22(4) artiklan mukaan automatisoidun päätöksenteon ja profiloinnin toteuttamiseksi suoritetut päätökset eivät saa perustua henkilötietojen erityisryhmiin kuuluviin tietoihin, ellei asianmukaisia toimenpiteitä rekisteröityjen suojelemiseksi ole suoritettu. Lisäksi tiettyjen poikkeussäännösten tulee soveltua tapaukseen. Toisin sanoen käsittelyn tulee perustua tärkeään yleiseen etuun ja käsittelyllä saavutettavan yleiselle edulle muodostuvan hyödyn tulee olla suhteellisuusperiaatteen mukaisesti oikeassa suhteessa käsittelyn tavoitteeseen nähden. Toinen poikkeustilanne, jolloin henkilötietojen erityisryhmiin kuuluvia tietoja saa hyödyntää profiloinnissa ja automatisoidussa päätöksenteossa, on käsillä, mikäli rekisteröity on antanut tähän nimenomaisen suostumuksen. Tällöin kuitenkin jäsenvaltion lainsäädännössä voi olla säännös, ettei pääsäännön mukaista kieltoa voida kumota edes rekisteröidyn suostumuksella. Tällainen kielto sisältyy muun muassa yksityisyyden suojasta työelämässä annetun lain 3.1 §:n ja 3.2 §:n mukaiseen tarpeellisuusvaatimukseen. Säännöksen mukaan työnantaja saa käsitellä vain välittömästi työsuhteen kannalta tarpeellisia työntekijöiden henkilötietoja, eikä tarpeellisuusvaatimuksesta voida poiketa edes työntekijän suostumuksella. Tämän poikkeuksen voidaan nähdä perustuvan heikomman suojan periaatteeseen, jolloin on katsottu, ettei tällainen työntekijän antama suostumus perustu välttämättä hänen vapaaseen tahtoonsa.

[326] Linder 2016, s. 38—41.

Yhteenvetona voidaan todeta, että profiloinnin sekä automaattisen päätöksenteon tulee aiheuttaa merkittäviä oikeusvaikutuksia rekisteröidylle, jotta näiden toimenpiteiden lähtökohtainen kielto olisi sovellettavissa. Tällöin käsittely on sallittua ainoastaan edellä kuvattujen poikkeuksien käsillä ollessa. Esimerkiksi profilointiin perustuvalla markkinoinnilla ei ole välttämättä merkittävää vaikutusta rekisteröidyn oikeudelliseen asemaan, ellei se ole poikkeuksellisen tunkeilevaa tai markkinointikanava ole poikkeuksellinen rekisteröidyn odotusten ja toiveiden näkökulmasta taikka markkinoinnin kohde ole erityisen haavoittuva. Viimeksi mainitussa, kyse voi olla erityisesti lapsiin kohdistuvasta markkinoinnista.

Lopuksi on syytä huomata, ettei automatisoitua päätöksentekoa koskevia säännöksiä voi kiertää näennäisellä ihmisosallisuudella. Jotta kyse ei olisi automatisoidusta päätöksenteosta tai profiloinnista, ihmisosallisuuden on tosiasiallisesti vaikutettava päätöksenteon lopputulokseen.[327] Edellä mainituista syistä voidaan todeta, että automatisoidun päätöksenteon tai profiloinnin käsillä ollessa rekisterinpitäjää sitovat tiukemmat osoitusvelvollisuutta koskevat velvoitteet.[328]

### 4.1.4. Rikoksiin ja rikkomuksiin liittyvien henkilötietojen käsittely

Yleisen tietosuoja-asetuksen 10 artiklan mukaan *”rikostuomioihin ja rikkomuksiin tai niihin liittyviin turvaamistoimiin liittyvien henkilötietojen käsittely 6 artiklan 1 kohdan perusteella suoritetaan vain viranomaisen valvonnassa tai silloin, kun se sallitaan unionin oikeudessa tai jäsenvaltion lainsäädännössä, jossa säädetään asianmukaisista suojatoimista rekisteröidyn oikeuksien ja vapauksien suojelemiseksi.”* Lisäksi säännöksessä todetaan, että kattavaa rikosrekisteriä voidaan pitää ainoastaan viranomaisen valvonnassa. Näin ollen tietosuoja-asetuksen yleisten käsittelyn oikeusperusteiden käsillä ollessa rikoksiin ja rikkomuksiin liittyviä henkilötietoja voidaan käsitellä ainoastaan viranomaisen valvonnassa tai kun unionin oikeus tai jäsenvaltion lainsäädäntö sen erikseen sallii, jolloin asianmukaisista suojatoimista on myös erikseen säädettävä.[329]

Henkilötietodirektiivin voimassa ollessa rikoksiin ja rikkomuksiin liittyvät henkilötiedot kuuluivat arkaluonteisten henkilötietojen joukkoon ja niiden käsittely oli lähtökohtaisesti kielletty. Vastaava sääntely koskee tietosuoja-asetuksen voimaan tulemisen myötä henkilötietojen erityisryhmiin kuuluvia tietoja. Kuten edellä todetusta voi huomata, nyttemmin rikoksiin ja rikkomuksiin liittyvien henkilötietojen käsittely kuuluu eräänlaiseen välimaastoon, jossa näiden tietojen käsittelyä ei ole lähtökohtaisesti kielletty. Nykyisin käsittely sallitaan, sen ollessa lain mukaista asetuksen 6 artiklan

[327] Tietosuojavaltuutetun toimiston ohje: Automaattinen päätöksenteko ja profilointi.
[328] Tietosuojatyöryhmä, WP 251, s. 6.
[329] Huomaa myös tutkielman II osan 3.2. kappaleessa käsitelty unionin erityislainsäädäntö koskien rikostuomioihin ja rikkomuksiin liittyvien henkilötietojen käsittelemistä unionin alueella eli direktiivi (EU) 680/2016, joka koskee ennen kaikkea viranomaistoimintaa ja -yhteistyötä.

nojalla, kunhan käsittely tapahtuu viranomaisen valvonnassa tai erillisen säännöksen valtuuttamana. Kuitenkin silloinkaan käsittely ei saa olla laajamittaista ilman viranomaisvalvonnan olemassaoloa.

Lähtökohtaisesti henkilötietojen erityisryhmiin kuuluvien sekä rikostuomioihin ja rikkomuksiin liittyvien henkilötietojen käsittelyprosesseista on laadittava tietosuoja-asetuksen mukainen edellä kuvattu vaikutustenarviointi eli DPIA.[330] Vaikutustenarviointia koskevan tutkielman III osan 4.1.2.1. kappaleessa todetusti, voidaan vaikutustenarvioinnin laatimiskriteerien täyttyessä sen suorittamisesta poiketa, mikäli vaikutukset ollaan muutoin arvioitu riittävällä tavalla, ellei laista erikseen muuta johdu. Tällöin käsittelyn oikeusperusteena tulee kuitenkin olla lakisääteinen velvoite tai oikeutettu etu. Tietosuojalain 7.2 §:ssä kansallista liikkumavaraa on käytetty siten, että siinä viitatun saman lain 6.2 §:n 10-kohdan mukaisesti asianmukaisina toimenpiteinä näissä käsittelytapauksissa pidetään muun muassa tietosuoja-asetuksen 35 artiklan mukaisen vaikutustenarvioinnin laatimista. Näin ollen Suomen tietosuojaa koskevassa yleislaissa pidetään lähtökohtana DPIA:n laatimisvelvoitetta sen kriteerien täyttyessä myös silloin, kun käsittely perustuu jäsenvaltion lakiin, ellei sovellettavasta erityislaista muuta johdu. Käsittelyn perustuessa lakisääteiseen velvoitteeseen tai oikeutettuun etuun, rekisterinpitäjän harkintavalta DPIA:n laatimisvelvoitteen arvioimisessa ei siis ole niin laaja, mitä se olisi voinut olla tietosuoja-asetuksen sanamuodon myötä.

Rikostuomioita ja rikkomuksia koskevien henkilötietojen käsitteleminen voi perustua kansallisen lainsäädännön puitteissa julkisista hankinnoista ja käyttöoikeussopimuksista annetun lain[331] (*hankintalaki*, 1397/2016) 80 §:n mukaiseen pakolliseen poissulkemisperusteeseen. Tällöin hankintayksikön on vaadittava tarjoajaa toimittamaan hankintalain 88.1 §:n ja 86.1 §:n perusteella ajantasaiset todistukset pakollisen poissulkemisperusteen tutkimiseksi ennen hankintasopimuksen solmimista. Säännösten mukaan otetta rikosrekisteristä on pidettävä tällaisena todistuksena.[332] Rikostuomioihin ja rikkomuksiin liittyvien tietojen käsittelyn osalta on myös otettava huomioon julkisuuslaki. Sen mukaan rikosrekistereihin merkitty tieto on salassa pidettävää.[333]

Tiedonhallintalaissa sekä hankintalaissa on säännöksiä asianmukaisista suojatoimista rikostuomioita ja rikkomuksia koskevien tietojen käsittelyyn liittyen. Tällaisten tietojen siirtämistä on rajoitettu. Lisäksi rikosrekisteriotteita on lähtökohtaisesti mahdollista käsitellä vain paperimuodossa. Hankintayksikön on huolehdittava riittävästä tietoturvasta erityisin toimenpitein, mikäli rikosrekisteriotteita ryhdytään vastaanottamaan ja käsittelemään sähköisesti.[334] Hankintalaissa estetään myös

[330] Tietosuojavaltuutetun toimiston ohje: Rekisteröidyn oikeuksista poikkeaminen tieteellisen tai historiallisen tutkimuksen tai tilastoinnin yhteydessä.
[331] Laki perustuu Euroopan parlamentin ja neuvoston direktiiviin 24/2014/EU, 26.2.2014, julkisista hankinnoista ja direktiivin 18/2004/EY kumoamisesta.
[332] Ks. myös TEM:n opas, 4/2017, s. 4.
[333] Ibid. s. 14.
[334] Ibid. s. 15.

rikosrekisteriotteiden jäljentäminen ja tallentaminen hankintayksiköiden lisäksi ehdokkaiden ja tarjoajien toimesta. Näin ollen 12 kuukautta voimassa olevien rikosrekisteriotteiden keskitetty tallennus ehdokas- ja tarjoajayhteisössä ei ole lain nojalla mahdollista, vaikka se helpottaisikin toistuvaa asiointia hankintayksikön kanssa.[335] Henkilöllä on kuitenkin aina oikeus itse tallentaa oma rikosrekisteriotteensa myöhemminkin hyödynnettäväksi, mutta tämä ei voi tapahtua rekisterinpitäjän toimesta rekisteröidyn lukuun.

Mikäli rikosrekisteriote tilataan rekisterinpitäjän työntekijältä, tulee ottaa huomioon, mitä säädetään yksityisyyden suojasta työelämässä annetussa laissa. Kyseisen lain soveltamisalan ulkopuolelle jäävät yhtiöiden toimitusjohtajat sekä hallituksen jäsenet. YksTL:n 3 §:n mukainen tarpeellisuusvaatimus on tällöin aina otettava huomioon, jolloin käsittely ei voi perustua pelkästään työntekijän suostumukseen. Lain 4.1 §:n mukaan työntekijää koskevat henkilötiedot on kerättävä ensisijaisesti työntekijältä itseltään tai tämän suostumuksella muualta. Työnantaja saa käsitellä rikosrekisterissä olevia tietoja, kun viranomaistaho luovuttaa niitä työnantajalle tämän laissa säädetyn tehtävän suorittamiseksi tai kun työnantaja hankkii rikosrekisteritietoja työntekijän luotettavuuden selvittämiseksi siten, kun YksTL:n 4 §:ssä ja oikeudesta saada tietoja rikosrekisteristä säädetään rikosrekisterilaissa (770/1993).

YksTL:n 4.3 §:n perusteella henkilötietojen kerääminen työhön otettaessa ja työsuhteen aikana kuuluu yhteistoimintalain, yhteistoiminnasta valtion virastossa ja laitoksessa annetun lain (651/1988) sekä työnantajan ja henkilöstön välisestä yhteistoiminnasta kunnissa annetun lain (449/2007) tarkoittaman yhteistoimintamenettelyn piiriin. Näin ollen käsillä olevissa tapauksissa Suomen kansallisen lainsäädännön nojalla tulee täytetyksi edellä kuvattuun vaikutustenarviointiin liittyvä velvollisuus kuulla rekisteröityjä taikka rekisteröityjen edustajia DPIA:n kriteerit täyttävän käsittelyn osalta. Mikäli kansallisessa lainsäädännössä säädetyt toimenpiteet nähdään riittäviksi vaikutusten arvioimisen kannalta, ei DPIA:ta tarvitse välttämättä laatia ja erillistä rekisteröityjen kuulemista toimittaa sen tullessa täytetyksi jo yhteistoimintamenettelyn puitteissa.

On huomattava, että vaikutustenarvioinnin kriteereistä säädetään tietosuoja-asetuksen 35 artiklassa siten, että DPIA on laadittava ainakin, jos kyse on laajamittaisesta rikostuomioihin ja rikkomuksiin liittyvien henkilötietojen käsittelystä. Nähdäkseni useissa hankintalakiin perustuvissa tapauksissa tämä laajamittaisuuden edellytys ei täyty, koska edellä kuvatuin tavoin rekisterinpitäjä ei saa jäljentää hankintalain nojalla toimittamiaan rikosrekisteriotteita. Jos kuitenkin työnantaja hankkii säännönmukaisesti rikosrekisteriotteet työhönottovaiheessa tai työsuhteen aikana esimerkiksi rekisterinpitäjän toimialasta johtuen, voi laajamittaisuuden kriteeri täyttyä. Hankintayksiköille toimitet-

[335] TEM:n opas, 4/2017, s. 18.

tavien rikosrekisteriotteiden sekä työhön ottamisvaiheessa saatujen rikosrekisteriotteiden käsittelemisen taustalla on lakisääteiset velvoitteet ja yksilön luotettavuuden arvioiminen. Henkilötietojen ryhmien ohella, nämä käsittelyn tarkoitukset ovat siinä määrin samankaltaiset, että nähdäkseni tällaiset käsittelyprosessit ovat yhdistettävissä samaan vaikutustenarvioimiseen tietosuoja-asetuksen 35(1) artiklan mukaisesti. Mikäli kyse on työntekijän kelpoisuuden arvioimisesta, voidaan tätä tarkoitusta varten kerättyjen terveystietojenkin käsittely sisällyttää saman vaikutustenarvioinnin piiriin.

### 4.1.5. Henkilötietojen erityisryhmiin kuuluvien tietojen käsittely

Yleisen tietosuoja-asetuksen 9(1) artiklan mukaan sellaisten henkilötietojen käsittely on kielletty, mistä ilmenee rekisteröidyn

- rotu tai etninen alkuperä
- poliittinen mielipide tai uskonnollinen taikka filosofinen vakaumus
- ammattiliiton jäsenyys
- geneettinen tai biometrinen tieto yksilön tunnistamista varten
- terveyttä koskeva tieto
- seksuaalinen käyttäytyminen tai suuntautuminen.

Lista vastaa muutamia jo aikaisemmin käsiteltyjä poikkeuksia lukuun ottamatta sitä, mitä henkilötietodirektiivissä säädettiin arkaluonteisista henkilötiedoista, joiden käsitteleminen oli samaan tapaan lähtökohtaisesti kielletty. Vaikka *arkaluonteiset henkilötiedot* oli terminä *henkilötietojen erityisryhmät* -käsitettä kuvaavampi, käytän tätä uutta ilmaisua, välttääkseni sekaannuksen aikaisemman henkilötietodirektiivin sisällöllisten eroavaisuuksien takia.

Pelkästään tietosuoja-asetuksen 6 artiklan mukaisten käsittelyperusteiden nojalla henkilötietojen erityisryhmiin kuuluvia tietoja ei saa käsitellä. Kyseisten henkilötietojen käsitteleminen on poikkeuksellisesti mahdollista, mikäli jokin tietosuoja-asetuksen 9(2) artiklan kriteereistä täyttyy. Tämän lisäksi tietosuoja-asetuksen 9(4) artiklan nojalla jäsenvaltiot voivat ottaa käyttöön lisäehtoja sekä rajoituksia, jotka koskevat geneettisten ja biometristen tietojen sekä terveystietojen käsittelyä. Silloin, kun henkilötietojen erityisryhmiin kuuluvien tietojen käsitteleminen perustuu jäsenvaltion lainsäädäntöön, on tällaisessa lainsäädännössä erikseen säädettävä asianmukaisista suojatoimista tietosuojan varmistamiseksi.

Kuten todettu, sekä henkilötietojen erityisryhmiin kuuluvien että rikostuomioihin ja rikkomuksiin liittyvien tietojen käsittelyn osalta vaikutustenarvioinnin laatiminen voi tulla kysymykseen. Tällainen korkea riski voi olla käsillä esimerkiksi, jos tietojen joutuminen vääriin käsiin tai niiden oikeudeton hyödyntäminen voisi johtaa sosiaaliseen vahinkoon, mukaan lukien maineen menetyk-

seen.[336] Kuten rikostuomioihin ja rikkomuksiin liittyvien tietojen osalta, myös henkilötietojen erityisryhmiin kuuluvia henkilötietoja käsiteltäessä DPIA on laadittava ainakin, mikäli tällainen käsittely on laajamittaista. Jos tätä säännöstä tulkitaan historiallisen tulkintatavan keinoin, lainsäätäjän tahtona on tuskin kyseistä ilmaisua käyttäessään ollut tarkoittaa normaaleista työnantajavelvoitteista huolehtimista, ellei tällaisessa käsittelyssä ole otettu käyttöön uutta teknologiaa, josta muodostuu erityinen riski rekisteröidylle. Mikäli DPIA:n tarpeellisuus perustuu käsiteltävien henkilötietojen luonteeseen asetuksen 35(3)(b) artiklan mukaisesti ja käsittelyprosessien tarkoitukset ovat olennaisilta osin samat, voi yhdistetyn vaikutustenarvioinnin laatia useamman tällä tavoin samankaltaisen käsittelyprosessin osalta.

On huomattava, että tietosuoja-asetuksen 88 artiklan nojalla jäsenvaltioille on annettu laajahkoa liikkumavaraa työsuhteen yhteydessä tapahtuvan käsittelyn osalta. Tällainen erityissääntely voi olla lakisääteistä taikka työehtosopimuksista johtuvaa. Esimerkiksi tietyissä työehtosopimuksissa on saatettu sopia siitä, että työnantaja pidättää ammattiliittoon kuuluvan työntekijän palkasta tämän jäsenmaksuosuuden ja tilittää sen ammattiliitolle.[337] Nähdäkseni tällainen toimenpide on jatkossakin mahdollista, kunhan järjestely on sopusoinnussa sovellettavan lainsäädännön sekä työehtosopimuksen kanssa, vaikka ammattiliiton jäsenyys onkin henkilötietojen erityisryhmiin kuuluva tieto. Tällainen käsittely ei tapahdu rekisterinpitäjän, vaan rekisteröidyn intressien nojalla. Yksityisyyden suojasta työelämässä annetussa laissa on säädetty tarkentaen muun muassa työsuhteen perusteella tapahtuvasta terveystietojen käsittelystä. Säännösten tulkinnassa voi pitkälti käyttää hyödyksi ennen GDPR:n sovellettavaksi tulemista syntynyttä oikeuskäytäntöä ja kirjallisuutta, sillä tässä suhteessa lakiin ei tullut juurikaan muutoksia EU:n tietosuojauudistuksen myötä.

### 4.2. Sisäänrakennettu ja oletusarvoinen tietosuoja

*Luottamuksellisuudesta*[338] yleisen tietosuoja-asetuksen johdanto-osan 39 kappaleessa korostetaan sitä, että tulee erityisesti ehkäistä luvaton pääsy henkilötietoihin sekä sellaisten laitteiden luvaton käyttö, joilla on mahdollista käsitellä henkilötietoja. Tällaisiin tilanteisiin tulee varautua erityisesti sisäänrakennetulla ja oletusarvoisella tietosuojalla. Sisäänrakennetun ja oletusarvoisen tietosuojan täyttämiseksi on suositeltavaa, että esimerkiksi ohjelmistohankintojen yhteydessä jo näitä koskevassa suunnitteluvaiheessa laaditaan suunnitelma tietosuojan oletusarvoisuuden ja sisään rakentamisen varmistamiseksi.[339]

---

[336] Tietosuojavaltuutetun toimiston ohje: Arvioi riskit ja suunnittele toimenpiteet tietosuojan toteuttamiseksi.
[337] Ks. esim. Yrittäjät, 23.10.2018: Työoikeuden professori Seppo Koskisen kannanotto sekä Yrittäjät, 21.2.2017: Suomen Yrittäjien lainopillisen asiamiehen Albert Mäkelän kannanotto.
[338] Luottamuksellisuus on tietoturvallisuuden periaatteen toinen elementti eheyden ohella.
[339] Huomaa myös Koski 2017, s. 49, jossa osuvasti todetaan, että sisäänrakennetun ja oletusarvoisen tietosuojan varmistamisessa on huomioitava käyttöönotetussa järjestelmässä tapahtuvan käsittelyn luonne. Esimerkiksi lapsiin kohdistuvassa käsittelyssä vaatimus asettaa sitä tiukempia suunnitteluvelvoitteita mitä nuorempiin rekisteröityihin käsittely kohdistetaan.

Jo edellä sivutun sisäänrakennetun tietosuojan periaatteen tulee ilmetä rekisterinpitäjän toiminnassa siten, että kaikki yleisen tietosuoja-asetuksen 5(1) artiklassa mainitut tietosuojaperiaatteet otetaan osaksi jokaista henkilötietojen käsittelyä sisältävää toimintoa. Sisäänrakennetun tietosuojan periaate kohdistuu konkreettisemmin henkilötietojen käsittelyä sisältäviin toimintoihin, kuten tietoteknisten järjestelmien toimintamekanismeihin. Käsiteltävien tietojen tulee tällöin olla tarpeellisia määrältään sekä käsittely ei saa ulottua laajuudeltaan pidemmälle kuin on tarpeen ja toisaalta säilytysajat on määriteltävä riittävän lyhyiksi. Tietojen tulee lisäksi olla saatavilla organisaatiossa vain sellaisilla henkilöillä, joilla voidaan katsoa esimerkiksi työtehtäviensä perusteella olevan asiallinen peruste näiden tietojen käsittelemiseksi.[340]

Sisäänrakennetun tietosuojan vaatimus edellyttää rekisterinpitäjältä myös käsittelytapojen määrittelyä ja tietosuojaperiaatteiden täytäntöönpano huomioon ottaen *riittäviä teknisiä ja organisatorisia toimenpiteitä*, joilla viitataan erityisesti henkilöstön kouluttamiseen ja eri keinoin tapahtuvaan riittävään valvontaan sekä tietoturvaan. Myös salassapitositoumukset voivat olla tarpeen, mikäli tietojen luovuttamisen edellytykset täyttyvät ja tietoja siirretään kolmansille osapuolille. Järjestelmän on lisäksi oltava sellainen, että tarvittaessa tietojen anonymisoimisointi ja pseudonymisointi sekä siirtäminen ei-aktiiviseen tilaan on mahdollista.

Sisäänrakennettu ja oletusarvoinen tietosuoja tarkoittaa täyttyessään sitä, että rekisterinpitäjä on huomioinut tietosuojakysymykset sekä tunnistanut riskit jo henkilötietojen käsittelyä sisältävien toimintojen suunnitteluvaiheessa eli tietosuojaperiaatteita on noudatettava käsittelyn alusta saakka[341]. Tämä periaate johtaa siihen, että rekisterinpitäjä ei enää voi vedota järjestelmässä oleviin puutteisiin ja näin välttyä tietosuojaperiaatteiden asettamilta vaatimuksilta. Tämä johtuu siitä, että rekisterinpitäjän on jo ennakolta tullut varmistua järjestelmien täyttävän kaikki tietosuojavaatimukset ja toimivan kaikkien tietosuojaperiaatteiden mukaisesti.[342]

### 4.3. Tietotilinpäätös

Kuten osoitusvelvollisuutta käytännössä koskevan 4. luvun alussa todetaan, yksi tapa täyttää osoitusvelvollisuus on laatia tietotilinpäätös, joka syntyy organisaation sisäisen auditoinnin tuloksena ja jossa kiinnitetään huomio rekisterinpitäjän henkilötietojen käsittelyn keskeisiin osiin. Lisäksi henkilötietojen käsittelijöiden toimintaa olisi säännöllisesti auditoitava rekisterinpitäjän toimesta

[340] Oikeusministeriön selvityksiä ja ohjeita, 4/2017, s. 13; Huomaa myös Euroopan komissio: Mitä tarkoittaa ’sisäänrakennettu’ ja ’oletusarvoinen’ tietosuoja?, jonka mukaan oletusarvoinen tietosuoja tarkoittaa erityisesti sitä, etteivät henkilötiedot ole oletusarvoisesti rajoittamattoman henkilöpiirin käytettävissä.
[341] Euroopan komissio: Mitä tarkoittaa ’sisäänrakennettu’ ja ’oletusarvoinen’ tietosuoja?
[342] Ks. Oikeusministeriön selvityksiä ja ohjeita, 4/2017, s. 13—14.

sekä huolehdittava EU/ETA:n ulkopuolelle tapahtuvaa tiedonsiirtoa koskevien erityisten vaatimusten täyttymisestä. Myös ulkoistetut henkilötietojen käsittelyprosessit kuuluvat rekisterinpitäjän käsittelytoiminnan piiriin.[343]

Johtopäätöksenä edellisistä kappaleista voidaan todeta tietotilinpäätöksen sisällöksi muodostuvan ensinnäkin tietojenkäsittelyohjeiden auditoinnin. Tietojenkäsittelyohjeisiin sisältyy muun muassa säilytyksen rajoittamisperiaatteen nojalla laadittu ohje henkilötietojen säilyttämisestä ja säilytysajoista. Organisaation on lisäksi tilanteen mukaan koulutettava henkilöstöään ja annettava yleisempiäkin ohjeita siitä, miten organisaatiossa tulee käsitellä henkilötietoja. Tietojenkäsittelyohjeiden kategoriaan kuuluvat myös rekisterinpitäjän ulkopuoliselle henkilötietojen käsittelijälle antamat ohjeet tietojen käsittelyä varten. Nämä kaikki dokumentit tulee olla yhtiön ylimmän johdon hyväksymiä ja säännöllisesti auditoituja. Tietosuojaohjeiden auditoimisessa on kyse yhtiön tietosuojaviestinnän tarkastamisesta, pitäen sisällään myös rekisteröityjen informoinnin ajantasaisuuden ja kielellisen selkeyden sekä yksinkertaisuuden varmistamisen. Tietosuojaa koskevan niin ulkopuolisiin kuin organisaation sisäisiin tahoihin kohdistuvan ohjeistuksen ei tulisi olla saatavilla tarpeettoman hajanaisesti useassa eri lähteessä.[344]

Tietotilinpäätöksen alaan kuuluvat myös tietojenkäsittelyprosessit sekä niiden dokumentoiminen. Tällöin organisaation olisi laadittava sisäänrakennetun ja oletusarvoisen tietosuojan vaatimusten soveltamiseksi suunnitelma (*Privacy by Design*) kyseisten velvoitteiden täyttämisestä aina, kun rekisterinpitäjä ottaa käyttöön uusia järjestelmiä, joissa käsitellään henkilötietoja. Tietojenkäsittelyprosessien auditoimiseen voi liittyä myös tietojenkäsittelysopimusten ja niihin liittyvien spesifikaattien auditoiminen. Lisäksi käsittelyperusteet[345] sekä rekisteröityjen ryhmät ja henkilötietojen kategoriat on dokumentoitava prosessikohtaisesti.[346]

Analogisesti ajateltuna, kun kirjanpitovelvollisen on säilytettävä tilikarttaa, jotta tilinpäätös voidaan asianmukaisesti suorittaa, olisi rekisterinpitäjällä oltava prosessikaavio, josta ilmenee kaikki rekisterinpitäjän tietojenkäsittelyprosessit. Tällaisen kaavion pohjalta voi saada paremman yleiskuvan rekisterinpitäjän tietojenkäsittelytoiminnasta sekä toteuttaa auditoinnit siten, ettei tietyt prosessit jää unohdetuiksi. Lisäksi tällaisen prosessikaavion avulla on kohdennettavissa paremmin rekisterinpitäjän ylimmän johdon antamat käsittelyohjeet. Auditoinnin tarkoituksena on myös varmistaa, että tietojenkäsittelyprosessit toimivat annettujen ohjeiden sekä sovellettavan lainsäädännön edellyttämällä tavalla.

---

[343] Lothermann 2017, s. 39—45, 90 ja 151 ja Kennedy et al. 2017, s. 45.
[344] Lothermann 2017, s. 59, 68, 96 ja 99 ja Kennedy et al. 2017, s. 109—114.
[345] Tällöin myös oikeutetun edun perustana oleva tasapainotesti tulee auditoiduksi.
[346] Lothermann 2017, s. 1—3, 59 ja 64; Carey et al. 2018, s. 240—248.

Lisäksi tietotilinpäätöksen suorittamiseksi organisaation on dokumentoitava tietojenkäsittelytoimet. Tällaisessa dokumentaatiossa mennään tietojenkäsittelyprosesseja yksityiskohtaisemmalle tasolle. Jotta prosessikohtaisten ohjeiden ja määritysten, mukaan lukien sisäänrakennettua ja oletusarvoista tietosuojaa koskevien suunnitelmien, mukaisuus voidaan varmistaa, edellyttää tämä myös dokumentaatiota siitä, millä tavalla henkilötietoja käsittelevät yksilöt, kuten organisaation työntekijät, ovat käsitelleet henkilötietoja. Edellä mainittu dokumentaatio koostuu eri järjestelmiin tallentuvista lokitiedoista ja varsinaisista henkilötiedoista, niistä tallentuvine metatietoineen sekä rekisteröidyiltä pyydettyjen suostumusten hallinnasta. Metatietojen avulla on varmistettavissa, ettei rekisterinpitäjä säilytä tarpeettoman vanhoja henkilötietoja. Lokitietojen avulla on puolestaan varmistettavissa, etteivät henkilötietojen käsittelijät kajoa tarpeettomiin henkilötietoihin ja toisaalta pääsy on rajoitettu riittävällä tavalla järjestelmän spesifikaateissa. Pääsyn rajoittaminen riittävällä tavalla on käsittelyprosessikohtainen asia, jonka käytännön toimivuus on auditoitavissa käsittelytoimia koskevan dokumentaation avulla.[347]

Rekisterinpitäjän on lisäksi dokumentoitava kaikki tietoturvan ja täsmällisyyden nimissä riskiperusteisesti suoritetut toimenpiteet. Tällaisia toimenpiteitä ovat toimet, joihin on ryhdytty rekisteröityjen käyttämien oikeuksien nojalla. Tietoturvatoimenpiteitä saatetaan suorittaa prosessikohtaisesti, mutta tällaisista toimista huolehditaan monesti myös laajemmalla tasolla. Konsernilla saattaa olla yhteinen portaali rekisteröityjen oikeuksien käyttämiseksi. Lisäksi rekisterinpitäjät saattavat huolehtia palomuurein ja muilla mahdollisilla tietoturvatoimenpiteillä tietokantojen ja tietovarantojen turvallisuudesta. Myöskään henkilötietojen eheyden takaamiseksi suoritettua varmuuskopiointia ei tule unohtaa.[348]

On huomattava, että rekisterinpitäjällä saattaa olla esimerkiksi samoilla verkkolevyillä tai muissa tietokannoissa useisiin eri käsittelyprosesseihin liittyviä henkilötietoja. Lisäksi yhtiön sisäisen ja ulkoisen viestinnän luottamuksellisuus on tässä suhteessa yksi olennainen elementti. Viestinnän luottamuksellisuudella ei kuitenkaan suojata ainoastaan yksilöä vaan myös oikeushenkilöä oikeussubjektina. Luottamuksellisuudesta sekä henkilötietojen täsmällisyydestä on huolehdittava asianmukaisin teknisin ja organisatorisin toimenpitein. Tietoturvatoimenpiteiden dokumentoimisen avulla sanottua asianmukaisuutta voidaan säännöllisesti arvioida. Tietoturvatoimien dokumentoinnista on kyse myös vaikutustenarviointien laatimisessa sekä ennakkokuulemisen suorittamisessa ja näiden toimenpiteiden dokumentoimisessa. Myös oikeutettuun etuun perustuvaa käsittelyä edeltävä tasapainotesti saattaa sisältää tarpeellisten tietoturvatoimien kuvauksia, joiden käytännön noudattaminen on auditoinnin kohteena.[349]

---

[347] Lothermann 2017, s. 64 ja 78—89.
[348] Ibid. s. 59—67, 140 ja 159.
[349] Ibid. s. 59—67, 140 ja 159.

Koska tietoturvaloukkauksiin liittyvästä ilmoitusvelvollisuudesta ja sitä kautta niihin liittyvästä dokumentoinnista on tietosuoja-asetuksessa erityissäännöksiä, käsittelen kyseistä kokonaisuutta seuraavaksi erikseen omassa kappaleessa. Tietoturvaloukkauksien dokumentoimisessa ja tämän dokumentoinnin auditoimisessa on kuitenkin kyse ainoastaan yhdestä tietotilinpäätöksen laajuuteen kuuluvasta osa-alueesta tietojenkäsittelyohjeiden, -prosessien, -toimien ja tietoturvatoimenpiteiden dokumentoimisen ohella.[350]

### 4.4. Tietoturvaloukkauksien dokumentoiminen

Tietosuoja-asetuksen mukainen riskilähtöisyys ilmenee asetuksen tietoturvaloukkauksien[351] ilmoitusvelvollisuutta koskevassa sääntelyssä. Ilmoitusvelvollisuuden täyttymistä tulee arvioida yksilön oikeuksiin ja vapauksiin kohdistuvan riskin todennäköisyyden näkökulmasta. Jos arvioinnissa päädytään siihen, että tietoturvaloukkauksesta aiheutuva riski ei ole todennäköinen, ei rekisterinpitäjän tarvitse ilmoittaa tietoturvaloukkauksesta rekisteröidylle tai valvontaviranomaiselle. Tietosuoja-asetuksessa rekisteröidyn oikeuksilla ja vapauksilla tarkoitetaan oikeutta henkilötietojen suojaan ja yksityisyyteen. Sillä viitataan myös muihinkin perusoikeuksiin, kuten liikkumisvapauteen, ajatuksenvapauteen, sananvapauteen, uskonnon ja omantunnon vapauteen, syrjinnän kieltoon sekä itsemääräämisoikeuteen. Myös yksilön omaisuuden suojalle eli rekisteröidylle muodostuva taloudellinen riski on otettava huomioon.[352] Yhtä kaikki ilmoitusvelvollisuutta koskeva arviointi on osoitusvelvollisuuden puitteissa dokumentoitava, vaikka tietosuojaviranomaiseen tai rekisteröityyn kohdistuvan ilmoitusvelvollisuuden kriteerit eivät täyttyisikään.

Velvollisuus ilmoittaa tietosuojaviranomaiselle[353] tietoturvaloukkauksesta edellyttää olosuhteita, joissa rekisteröidyn oikeuksille ja vapauksille kohdistuvan riskin todennäköisyys on olemassa. Näin ollen nähtävissä olevan riskin olemassa oleminen on riittävä täyttääkseen kyseisen ilmoitusvelvol-

---

[350] Lothermann 2017, s. 154 ja Carey et al. 2018, s. 88—101.

[351] GDPR:n 4 artiklan 12-kohdan mukaan tietoturvaloukkauksella tarkoitetaan tilannetta, *"jonka seurauksena on siirrettyjen, tallennettujen tai muuten käsiteltyjen henkilötietojen vahingossa tapahtuva tai lainvastainen tuhoutuminen, häviäminen, muuttaminen, luvaton luovuttaminen taikka pääsy*". Kyse voi olla esimerkiksi rekisterinpitäjän työntekijän päätelaitteen, kuten työssä käytetyn kannettavan tietokoneen, katoamisesta tai kyberhyökkäyksestä.

[352] Tietosuojatyöryhmän ohje, WP 248, s. 7.

[353] Tietoturvaloukkauksesta tehtävä ilmoitus Suomen tietosuojaviranomaiselle on suoritettavissa seuraavan linkin kautta aukeavalla lomakkeella: https://tietosuoja.fi/ilmoitus-tietoturvaloukkauksesta. Sikäli kun tietoturvaloukkaus kohdistuu sähköisen viestinnän palveluun, voi olla aiheellista tehdä ilmoitus myös Liikenne- ja viestintävirasto Traficomin alaiselle kyberturvallisuuskeskukselle seuraavan linkin kautta: https://www.kyberturvallisuuskeskus.fi/fi/ilmoita. Kyberturvallisuuskeskukselle tehtävä ilmoitus ei ole yhteisötilaajalle välttämätön toimenpide tietoturvaloukkauksen käsillä ollessa, mutta se voi olla aiheellinen osoitusvelvollisuuden puitteissa. Rikoslain 38:8:n sekä 38:8a:n mukaisen tietomurron tai törkeän tietomurron sekä 38:9:n mukaisen tietosuojarikoksen käsillä ollessa myös rikosilmoituksen tekeminen poliisille on aiheellista. Jälkikäteen arvio kohdistuu osoitusvelvollisuuden puitteissa nimenomaisesti siihen, että rekisterinpitäjä on ryhtynyt tietoturvaloukkauksen johdosta kaikkiin tarpeellisiin toimenpiteisiin asian selvittämiseksi sekä vahinkojen ehkäisemiseksi taikka lisävahinkojen vähentämiseksi.

lisuuden edellytykset. Sen sijaan rekisteröidylle tietoturvaloukkauksesta tulee ilmoittaa, kun todennäköisyys yksilön oikeuksille ja vapauksille kohdistuvalle korkealle riskille on olemassa sekä mikäli tietyt asetuksessa erikseen määritellyt poikkeukset[354] eivät täyty.[355]

Tietosuojaviranomaiselle ilmoittamisen osalta ei ole säädetty vastaavalla tavalla poikkeuksia. Rekisteröityyn kohdistuvan ilmoitusvelvollisuuden kynnys on siis korkeampi. Tätä on perusteltu tietosuoja-asetuksen laatimisvaiheessa muun muassa sillä, että pyritään välttämään sellaisen tilanteen muodostumista, jossa rekisteröidyt saavat päätelaitteensa täyteen ilmoituksia kaikenlaisista riskeistä. Tällöin todellisiin uhkiin ei enää reagoitaisi tai rekisteröidyn olisi ainakin hankala arvioida, milloin on tosiasiallisesti käsillä sellainen tilanne, johon olisi välittömästi reagoitava. On huomattava, että rekisteröidylle tehtävän ilmoituksen on oltava henkilökohtainen, mikä voidaan toteuttaa esimerkiksi tietoturvaloukkauksen vaikutuspiiriin kuuluville rekisteröidyille kohdennetulla sähköpostilla, mikäli se on mahdollista.

Osoitusvelvollisuuden täyttämiseksi rekisterinpitäjän on dokumentoitava jokaisen tietoturvaloukkauksen olosuhteet sekä siitä aiheutuneet seuraukset ja olemassa olevat riskit. Lisäksi rekisterinpitäjän on kirjattava tietoturvaloukkauksen johdosta tehdyt korjaavat toimenpiteet. Edellä mainitun lisäksi tietoturvaloukkaukseen liittyen on tapauksen mukaan dokumentoitava selvitys siitä, mikäli tietoturvaloukkauksesta on päädytty ilmoittamaan tietosuojaviranomaiselle. Jos tämän lisäksi tietoturvaloukkauksesta on ilmoitettu rekisteröidylle, myös sitä koskevan korkean riskin täyttymisestä on dokumentoitava selvitys[356]. Näin syntynyt aineisto on auditoitava säännöllisesti, jotta voidaan varmistaa, että tietoturvaloukkauksien johdosta on ryhdytty kaikkiin tarpeellisiin toimenpiteisiin.[357]

### 4.5. Sertifiointimekanismit, hyväksytyt käytännesäännöt ja selosteet

Yksi keino osoitusvelvollisuuden täyttämiseksi, on käyttää tietosuojaa koskevia tietosuoja-asetuksen mukaisia sertifikaatteja ja käytännesääntöjä, joilla voidaan osoittaa rekisterinpitäjän noudattavan tietosuojavelvoitteitaan. *Sertifikaateista* säädetään tietosuoja-asetuksen 42 artiklassa sekä johdanto-osan 100 kappaleessa ja niiden tarkoituksena on antaa rekisterinpitäjälle paremmat mahdol-

---

[354] GDPR:n 34(3) artiklan mukaan rekisteröidylle ei tarvitse ilmoittaa tietoturvaloukkauksesta, jos
- rekisterinpitäjä on toteuttanut asianmukaiset tekniset ja organisatoriset suojatoimenpiteet ja tietoturvaloukkauksen kohteena oleviin tietoihin on sovellettu kyseisiä toimenpiteitä, erityisesti, mikäli niiden avulla henkilötiedot on pseudonymisoitu
- rekisterinpitäjä on toteuttanut jatkotoimenpiteitä, joilla varmistutaan siitä, että rekisteröityjen oikeuksiin ja vapauksiin kohdistuva korkea riski ei enää todennäköisesti täyty
- se vaatisi kohtuutonta vaivaa.

Viimeksi mainitussa tilanteessa on kuitenkin käytettävä julkista tiedonantoa tai muuta vastaavaa toimenpidettä, jolla rekisteröidyille tiedotetaan yhtä tehokkaalla tavalla.

[355] Andersson 2018, s. 7 ja Carey et al. 2018, s. 88—98.

[356] Toisaalta selvityksestä on ilmettävä myös perusteet sille, miksi korkea riski ei täyty, mikäli rekisteröidyille ei ole ilmoitettu tietoturvaloukkauksesta.

[357] Article 29 Data Protection Working Party, WP 250, s. 23—25.

lisuudet arvioida palveluiden ja tuotteiden tietosuojatasoa. GDPR:n rekisterinpitäjän vastuuta koskevassa 25(3) artiklassa todetaan suoraan, että sertifiointimekanismien käyttöönottaminen voi olla yksi tekijä osoitusvelvollisuuden täyttämisessä, joten ne on otettava huomioon tietosuojaviranomaisen arvioidessa osoitusvelvollisuuden täyttymistä. *Käytännesäännöistä* puolestaan säädetään tietosuoja-asetuksen 40—41 artikloissa sekä johdanto-osan 98—99 kappaleissa. Ne ovat tarkoitettu alakohtaisiksi, jolloin huomioiduksi tulevat eri aloilla tapahtuvan käsittelyn erityispiirteet ja näin tietosuoja-asetuksen soveltaminen helpottuu.[358]

Yhteenvetona voidaan todeta, että sertifiointimekanismeilla on suuri vaikutus osoitusvelvollisuuden täyttämisessä, koska näihin mekanismeihin sisältyy pääsääntöisesti auditointia, jonka läpäiseminen edellyttää kyvykkyyttä osoittaa tietosuojaperiaatteiden noudattamista. GDPR:n 35(8) artiklan mukaan hyväksytyillä käytännesäännöillä on puolestaan merkitystä etenkin DPIA-menettelyssä. Tämä johtunee siitä, että käytännesääntöjen laatiminen perustuu organisaatio- tai toimialakohtaisesti käsillä olevien riskien arvioimiseen.

Keskeisenä keinona tietosuojaperiaatteiden noudattamisen osoittamiseksi voidaan pitää myös *selosteita*, joista säädetään tietosuoja-asetuksen 30 artiklassa ja johdanto-osan 82 kappaleessa. Tällöin rekisterinpitäjät sekä henkilötietojen käsittelijät laativat selosteita vastuullaan olevista käsittelytoimista. Selosteiden on oltava kirjallisessa muodossa, jotta osoitusvelvollisuus täyttyy, ja tietosuojaviranomaisella on oikeus saada nämä selosteet nähtävilleen pyynnöstä. Kaikkien organisaatioiden ei kuitenkaan tarvitse tällaisia selosteita laatia, jolloin toiminnanharjoittajan vastuulle jää arvioitavaksi, tarvitseeko tämän laatia selosteita.[359]

Näin ollen hyväksytyt käytännesäännöt ja sertifikaatit ovat vaihtoehtoisia keinoja suorittaa asianmukaisia teknisiä ja organisatorisia toimenpiteitä tietosuojavelvoitteiden täyttämiseksi. Yhtenä käytännöllisenä keinona tietoturvaperiaatteen sekä siihen liittyvän auditoinnin suorittamiseksi osoitusvelvollisuuden puitteissa voidaan mainita ISO/IEC 27001:2017[360] -standardin käyttöönottaminen. Kyseinen standardi sisältää määräykset tietoturvallisuuden hallintajärjestelmien luomiseksi, toteuttamiseksi, ylläpitämiseksi sekä jatkuvaksi parantamiseksi.[361] Näiden hallintajärjestelmien luomiseen vaikuttavat organisaation koko sekä tarpeet ja tavoitteet, joten käytännössä standardin käyttöönottaminen ja sen auditoiminen täyttävät pitkälti myös toimialakohtaiset erityisvaatimukset.[362]

[358] Oikeusministeriön selvityksiä ja ohjeita, 4/2017, s. 14.
[359] Ibid. s. 14.
[360] Eurooppalainen standardi ISO/IEC 27001:2017 ”Information technology. Security techniques. Information security management systems. Requirements (ISO/IEC 27001:2013 including Cor. 1:2014 and Cor 2:2015)”.
[361] ISO/IEC 27001:2017, s. 5.
[362] Ibid. s. 5.

Tietoturvallisuuden hallintajärjestelmien avulla on tarkoitus suojata tiedon eheyttä, luottamuksellisuutta sekä saavutettavuutta ja lisätä sidosryhmien välistä luottamusta. Mikäli rekisterinpitäjä päättää ulkoistaa tietojenkäsittelytoimintojaan, yksi keino varmistua siitä, että henkilötietojen käsittelijä noudattaa riittäviä tietoturvakäytäntöjä ja -politiikkaa on edellyttää, että kyseinen organisaatio on ottanut käyttöönsä ISO/IEC 27001:2017 -standardin. Tällöin tietojenkäsittelysopimuksen liitteenä ohjeistettujen tietoturvatoimenpiteiden ei välttämättä tarvitse olla yhtä kattavat kuin muussa tapauksessa, sillä käytännössä kyseisen standardin edellyttämät tietoturvakäytännöt täyttävät tällaisten liitteiden vakiosisällön.[363]

### 4.6. Jälkivalvonta

Eräs osoitusvelvollisuuden täyttämiseksi vaadittu toimenpide on *tietosuojavastaavan* nimittäminen, mikä ei ole pakollinen toimenpide kaikille organisaatioille. Alun perin komission ehdotuksen tietosuojavastaavaa koskevassa kohdassa todettiin, että tietosuojavastaava tulisi nimittää jokaiseen organisaatioon, jolla on vähintään 250 työntekijää. Tällöin velvoite olisi kohdistunut noin 40 %:n Euroopan unionin alueella toimivista yhtiöistä.[364] Valmistelutyön aikana sanamuoto muuttui siten, että nimittämisvelvollisuus koskisi kaikkia rekisterinpitäjiä, jotka käsittelevät vuodessa yli 500 rekisteröidyn henkilötietoja.[365] Viimeisimmässä parlamentin valmisteluaineistossa rajaksi asetettu kriteeri oli noussut 5000 rekisteröityyn 12 kuukauden ajanjaksolla.[366] Tietosuoja-asetuksen tietosuojavastaavan nimittämistä koskevaan 37 artiklaan ei lopulta jäänyt mitään numeerista kriteeriä nimittämisen edellytyksistä. Viimeisimpien valmisteluaineistojen mukainen ajatus siitä, että tietosuojavastaavan nimittämisen tarpeellisuutta pitäisi arvioida enemmänkin tietojenkäsittelytoiminnan luonteen ja laajuuden näkökulmasta, eikä henkilötietoja käsittelevien tahojen lukumäärästä käsin, jäi kuitenkin voimaan.[367]

Konserni[368] voi nimittää tietosuoja-asetuksen 37(2) artiklan mukaisesti yhden ainoan tietosuojavastaavan edellyttäen, että tietosuojavastaavaan on otettavissa helposti yhteyttä jokaisesta toimipaikasta. Tämä on yhdenmukaista myös tietosuoja-asetuksessa omaksutun *one-stop-shop* -periaatteen kanssa, minkä nojalla konserni voi valita tietyn jäsenvaltion tietosuojaviranomaisen johtavaksi valvontaviranomaiseksi ja näin ollen toimivaltaiseksi koordinoimaan organisaatioon kohdistuvia tietosuojaan liittyviä tutkintatoimia yhtiön päätoimipaikan tai muun sijoittautumisen perusteella.[369]

---

[363] ISO/IEC 27001:2017, s. 5—14.
[364] Korhonen 2016, s. 603.
[365] LIBE on the GDPR, s. 54: silloisesta 35 artiklasta.
[366] European Parliament on the GDPR, s. 54: silloisesta 35 artiklasta.
[367] Ks. GDPR:n 37 artiklan kriteerit tietosuojavastaavan nimittämiselle.
[368] GDPR:n 4 artiklan 19-kohdan mukaan konsernilla tarkoitetaan *"määräysvaltaa käyttävää yritystä ja sen määräysvallassa olevia yrityksiä"*.
[369] Article 29 Data Protection Working Party, WP 244, s. 4.

Yhtenä tietosuojavastaavan tehtävänä on asetuksen 39(1)(b) artiklan nojalla osallistua osoitusvelvollisuuden täyttämiseksi suoritettaviin auditointeihin, joiden on tapahduttava säännöllisin väliajoin tietosuojaperiaatteiden täyttämiseksi. Tietosuojavastaavan on osallistuttava sisäisten auditointien lisäksi myös viranomaisen jälkivalvonnan puitteissa tapahtuvaan auditoimiseen rekisterinpitäjän edustajana.[370] On myös huomattava, että tietosuojavastaava voi olla rekisterinpitäjään nähden ulkopuolinenkin taho.[371]

Käytän tutkielmassani tietosuojalainsäädännön mukaisesta riippumattomasta valvontaviranomaisesta nimitystä *tietosuojaviranomainen*. Yleisen tietosuoja-asetuksen 58(1)(b) artiklan mukaan tietosuojaviranomaisen valtuuksiin kuuluu toteuttaa tutkimuksia tietosuojaa koskevien tarkastusten muodossa. Tietosuojaviranomaisella on oikeus saada rekisterinpitäjältä sekä henkilötietojen käsittelijältä kaikki tehtäviensä suorittamiseksi tarpeelliset tiedot, mukaan lukien pääsyn kaikkiin henkilötietoihin tai muihin tarpeellisiin tietoihin taikka tiloihin ja tietojenkäsittelylaitteisiin.[372] Ennen kaikkea rekisterinpitäjän on kyettävä osoitusvelvollisuuden mukaisesti osoittamaan noudattavansa toiminnassaan sovellettavaa tietosuojalainsäädäntöä.

Mikäli rekisterinpitäjä ei ole kyennyt täyttämään osoitusvelvollisuuttaan taikka henkilötietojen käsittelijä ei ole kyennyt noudattamaan rekisterinpitäjän antamia ohjeistuksia, voi tietosuojaviranomainen antaa näille varoituksen tai huomautuksen. Lisäksi tietosuojaviranomainen voi antaa sitovia määräyksiä tietosuojavelvoitteiden noudattamiseksi ja asettaa väliaikaisia tai pysyviä rajoituksia käsittelylle sekä määrätä hallinnollisen sakon taikka peruuttaa sertifioinnin.[373] Auditoinnin yhteydessä tietosuojaviranomainen voi myös erikseen antaa hyväksyntänsä tietyille menettelyille tai vaihtoehtoisesti neuvoa rekisterinpitäjää ja henkilötietojen käsittelijää lievempänä toimenpiteenä.[374] Analogisesti voidaan huomata, että myös yhtiöiden kirjanpitoon liittyen dokumentaatio on vuotuisesti auditoitava. Säännöllistä auditointia edellytetään myös tietosuoja-asetuksen puitteissa. Viranomaisen suorittamat auditoinnit eivät ole kuitenkaan säännöllisiä, mutta yhtiöiden kirjanpitoon kohdistuvat viranomaisen suorittamat verotarkastuksetkaan eivät ole vuotuisia prosesseja.[375]

---

[370] GDPR:n 39(1)(d) ja 39(1)(e) artiklat tietosuojavastaavan ja tietosuojaviranomaisen yhteistyöstä.
[371] Korhonen 2016, s. 602.
[372] GDPR:n 58(1)(e) ja 58(1)(f) artiklat.
[373] GDPR:n 58(2) artiklassa on lueteltu mahdolliset tietosuojaviranomaisen toimenpiteet. Ks. lisäksi Tietosuojavaltuutetun toimiston tiedote, 1.3.2018, tietosuojavaltuutetun uusista tehtävistä.
[374] GDPR:n 58(3) artikla tietosuojaviranomaisen hyväksymis- ja neuvontavaltuuksista.
[375] On huomattava, että osakeyhtiöiden tilintarkastus on vuotuinen ei-viranomaisen, mutta kylläkin riippumattoman ulkopuolisen tahon suorittama prosessi. Tämän menettelyn lähelle päästäisiin, mikäli organisaatio nimittäisi itselleen ulkopuolisen auditointeihin osallistuvan tietosuojavastaavan. Joka tapauksessa myös organisaation sisälle nimetyn tietosuojavastaavan tulisi olla mahdollisimman riippumaton tietosuoja-asetuksen nojalla. Analogisesti todettakoon, että myöskään tilintarkastajaa ei saisi vaihtaa sen takia, että tämä pyrkii suorittamaan vastuullisesti tehtäviään.

### 4.6.1. Tietosuojaviranomaisen toimivalta seuraamusprosessissa

Tietosuojaviranomaisen jälkivalvonnassa havaittujen puutteiden johdosta valvontaviranomainen voi määrätä hallinnollisia sakkoja. Heti alkuun on syytä kiinnittää huomiota hallinnollisten sanktioiden ja rikosoikeussanktioiden väliseen problematiikkaan. *Ne bis in idem* -periaate[376] edellyttää, että ketään ei voida tuomita kahdesti samasta teosta. Tämä estää itseasiassa lähtökohtaisesti jo saman asian uudelleen tutkimisen, mikäli asialle on jo olemassa lainvoimainen päätös. Hallinnollisten sanktioiden ryhmään kuuluvassa hallinnollisessa sakossa on kyse julkisoikeudellisesta sanktiosta, rikosoikeudellisten sanktioiden tapaan. Näitä sanktioita ainoastaan käsitellään eri tuomioistuinlinjassa. Rikosprosessi kokonaisuutenakin ottaen on julkisen vallan käyttöä. Näin ollen ei ole perusteltua, että samasta teosta määrätään samalle taholle sekä rikosoikeudellinen että julkisoikeudellinen sanktio johtuen ne bis in idem -periaatteesta, sillä molemmissa tapauksissa kyse on julkista valtaa käyttäen määrätystä sanktiosta.[377]

Tietosuojaperiaatteiden rikkomisesta voi seurata myös siviilioikeudellinen vahingonkorvausvastuu. Tällaiset oikeustapaukset käsitellään yleisissä tuomioistuimissa[378], eikä tällöin ole kyse julkisoikeudellisesta sanktiosta, jolloin ne bis in idem -periaate ei sovellu. On kuitenkin mahdollista, että tällainen vaade yhdistetään adheesioperiaatteen nojalla rikosprosessiin. Tässä kohtaa käsittelyn kohteena on kuitenkin ennen kaikkea hallintoprosessi. Rikosprosessissa ei arvioida osoitusvelvollisuuden täyttymistä, vaan kyse on siitä, täyttyykö rikoksen tunnusmerkistö sekä siihen mahdollisesti liitetty tahallisuus tai tuottamus. Tietosuojarikoksesta voi tuomita ainoastaan, mikäli kyseessä on törkeä tuottamus tai tahallisuus. Hallintoprosessissa määrättävän hallinnollisen sakon edellytyksenä ei ole kuitenkaan törkeä tuottamus tai tahallisuus.

Kuten todettu, jäsenvaltioiden on asetettava kansallinen valvontaviranomainen valvomaan sekä yksityisellä että julkisella sektorilla tapahtuvaa tietojenkäsittelytoimintaa. Suomessa tämä tehtävä on

---

[376] Euroopan ihmisoikeussopimuksen seitsemännen lisäpöytäkirjan 4 artikla.

[377] Niemi 2015, s. 338 ja KHO 2011:41, KHO 2014:145, KKO 2010:45, KKO 2010:46, KKO 2013:59 sekä EIT:n ratkaisut Jussila v. Suomi, 23.11.2006 ja Zolotukhin v. Venäjä, 10.2.2009; Toisaalta Euroopan ihmisoikeustuomioistuin on hiljattain muuttanut linjaansa siitä, mitä kaikkea ne bis in idem -periaatteen piiriin kuuluvalla syytteellä tai rangaistuksella voidaan tarkoittaa (Mihalache v. Romania, 8.7.2019). Mikäli toimenpiteessä ei ole pohjimmiltaan kyse täysin samasta asiasta tai kyseessä ei ole suoranaisesti hallinnollinen tai rikosoikeudellinen sanktio taikka niihin liittyvä syyte, kuten myös korkeimman hallinto-oikeuden ratkaisussa KHO 2019:35 todetaan, ei ne bis in idem -periaate estä seuraamuksen määräämistä (hyvike perustui samaa tapausta koskevaan sopimukseen, eikä kyse ollut näin ollen ne bis in idem -periaatteen estämästä sanktiosta). Toisaalta jo pelkkä syyttämättäjättämispäätös johtaa vastaisuudessa ne bis in idem -periaatteen soveltamiseen (Mihalache v. Romania).

[378] On myös huomattava, että tietojenkäsittelysopimuksen mahdollisesti sisältämän välityslausekkeen nojalla tietosuoja-asetuksen mukainen rekisterinpitäjän ja henkilötietojen käsittelijän välinen regressioikeus, jolla konstruoidaan sopimuksen osapuolten siviilivastuuta (tarkemmin sanottuna sopimusvastuuta) osapuolien välillä, on käsiteltävissä välimiesoikeudessa. Välimiesoikeuden alaan ei ole kuitenkaan alistettavissa rekisteröidyn esittämiä vaateita siinä menettelyssä, jossa rekisteröity nimenomaisesti hakee itselleen korvauksia, sillä rekisteröity ei ole tällaisen sopimuksen osapuoli ja lisäksi GDPR:n 82 artiklan nojalla pakottavasti velvoitetaan, että yksilöllä on oltava oikeus hakea korvausta keneltä tahansa käsittelyyn osallistuneelta taholta.

osoitettu tietosuojavaltuutetun toimistolle, jonka johtajana toimiva tietosuojavaltuutettu sekä apulaistietosuojavaltuutettu voivat antaa tietosuojalainsäädäntöön perustuvia ratkaisuja ja päätöksiä sekä määrätä hallinnollisia seuraamusmaksuja seuraamuskollegion enemmistöpäätöksellä tietosuojalain 24 §:n mukaisesti. Tietosuojaviranomaisen ratkaisuista valitetaan hallintotuomioistuimiin.[379] Tutkielmani rajauksellisista syistä en tule johdannossa todettuun tapaan syventymään suomalaiseen lainsäädäntöön, vaan tarkastelu kohdistuu erityisesti unionin oikeuteen.

Tietosuojaviranomaisen tehtävänä on osana suorittamaansa jälkivalvontaa, kuten auditointeja, varmistaa, että rekisterinpitäjät noudattavat tietosuojalainsäädännön asettamia vaatimuksia ilmentäviä tietosuojaperiaatteita. Tämä on pystyttävä osoittamaan tietosuojaviranomaisille osoitusvelvollisuuden nojalla. Toisin sanoen rekisterinpitäjän on kyettävä osoittamaan tietosuojaviranomaiselle toimivansa vähintään tutkielmani III osiossa kuvatulla tavalla.[380]

On huomattava, että erityislainsäädäntöön kuuluvan tietosuojalainsäädännön noudattamisen valvonnassa tietosuojaviranomaisen toimivalta saattaa olla osin päällekkäistä muiden viranomaisten toimivallan kanssa. Tällainen tilanne on käsillä esimerkiksi sosiaali- ja terveysalalla[381]. Kansallisen lainsäädännön avulla on mahdollista selkeyttää vallitsevaa oikeustilaa tältä osin. Mikäli kyse on suoraan tietosuoja-asetukseen perustuvasta lainsäädännöstä, tulee tällaisen lainsäädännön noudattamisen valvonnan kuulua kansallisen tietosuojaviranomaisen toimivaltaan, vaikka kyse olisikin erityislainsäädännöstä.[382]

Tietosuojaviranomaisella on erittäin laajat valtuudet pyytää rekisterinpitäjältä dokumentaatiota osoitusvelvollisuuden noudattamisesta sekä lisäksi kaikkea muuta informaatiota, mikä voi olla tarpeen jälkivalvonnan tai viranomaiselle tehdyn valituksen tutkimiseksi. Käytännössä tietosuojaloukkaustilanteissa rekisterinpitäjä voi välttää vastuun muodostumisen ainoastaan, mikäli tämä on laatinut henkilötietoja käsitteleville luonnollisille henkilöille riittävät ohjeistukset sekä auditoinut niiden noudattamista riittäväksi katsotulla tavalla, mutta henkilötietoja käsitellyt taho on siitä huolimatta poikennut annetusta ohjeistuksesta. Sama pätee tilanteisiin, joissa henkilötietojen käsittelijä todetaan rekisterinpitäjän sijaan vastuulliseksi tietosuojaloukkauksesta.[383]

---

[379] Havainnollistavana esimerkkinä siitä, kuinka tietosuojalainsäädäntö voi tulla arvioitavaksi myös muidenkin viranomaisten kuin tietosuojaviranomaisen toimivaltuuksia arvioitaessa, on korkeimman hallinto-oikeuden ratkaisu KHO 2020:8, jossa verohallinnon verotusmenettelystä annetun lain (1558/1995) 21 §:n perusteella annettu kehotus pankille A Oyj toimittaa listaus kaikista asiakkaistaan vertailutietotarkastuksen suorittamista varten todettiin tietosuoja-asetukseen sekä tietosuojalain 4.1 §:n 2-kohtaan viitaten lain vastaiseksi. Näin ollen verohallinnon päätös kumottiin. Päätöksen liitteeksi otettiin tietosuojavaltuutetun lausunto, mutta asia ei kuitenkaan alun perin tullut vireille tietosuojaviranomaisen toimesta. Tietosuojavaltuutettu totesi lausunnossaan, että liian epätäsmällisesti kohdennettu tietopyyntö loukkasi yksilöiden henkilötietojen suojaa.

[380] Ks. esim. Adshead 2016, s. 120 ja 123.

[381] Alueellisesti AVI ja valtakunnallisesti Valvira.

[382] Adshead 2016, s. 121—122 ja 125. Lisäksi tällaisen lainsäädännön laatimisvaiheessa on kuultava tietosuojavaltuutettua.

[383] Ibid. s. 127.

Käytännössä osoitusvelvollisuuden täyttämiseksi relevantti dokumentaatio koostuu ilmoituksista, prosessikaavioista ja käsittelytoimia koskevasta dokumentaatiosta sekä politiikoista[384]. Myös vaadittavan riskienhallinnan osoittamiseksi rekisterinpitäjällä tulee olla dokumentaatiota.[385] Rekisterinpitäjän on myös kyettävä osoittamaan, että tämä auditoi säännöllisesti tietojenkäsittelytoimintaansa ja sen ohella myös henkilötietojen käsittelijöiden käsittelytoimintaa[386]. Lisäksi tietosuojavastaavan nimittämisen tarpeellisuutta on arvioitava, mikäli sellaista ei ole organisaatioon vielä nimetty ja vaikka tällainen olisikin nimetty, voidaan tarkastella, onko yhden tietosuojavastaavan nimittämistä konsernille pidettävä riittävänä toimenpiteenä. Tietosuojaviranomaisella on valtuudet ryhtyä tarkastuksiin joko oma-aloitteisesti taikka tietosuojaviranomaiselle tehdyn valituksen tai ilmoituksen johdosta.[387] Lisäksi tietosuojavaltuutetun toimivalta ulottuu Suomessa tietosuojalain 18.2 §:n nojalla jopa yksilön kotirauhan piiriin, mikäli on syytä epäillä tietosuojalainsäädäntöä rikotun hallinnollisen sakon määräämiseen johtavalla tavalla tai rikoslaissa säädetyn rikoksen tunnusmerkistön todennäköisesti täyttyessä.

Tietosuojaviranomainen voi seuraamuksina tehdä huomautuksia, toimenpidemääräyksiä, määräyksiä pidättäytyä tietystä toiminnasta sekä määrätä hallinnollisia sakkoja. Suomessa GDPR:n mahdollistaman liikkumavaran nojalla tietosuojalain 24.4 §:n mukaisesti seuraamusmaksua ei voida määrätä valtion viranomaisille, liikelaitoksille, kunnallisille viranomaisille, julkisoikeudellisille itsenäisille laitoksille, eduskunnan virastoille, tasavallan presidentin kanslialle, Suomen evankelis-luterilaiselle tai ortodoksiselle kirkolle eikä näiden seurakunnille, seurakuntayhtymille ja muille elimille. Kuitenkin muut tietosuojaloukkauksesta johtuvat määräykset on mahdollista kohdentaa myös edellä mainituille toimijoille.

Yleisen tietosuoja-asetuksen 83 artiklaan perustuen voidaan todeta, että hallinnollinen sakko on tarkoitettu viimesijaiseksi seuraamukseksi, eikä siihen tule ryhtyä kevyin perustein. GDPR:n 83(1) artiklan perusteella seuraamusmaksuun tulee ryhtyä ainoastaan, mikäli muita puuttumiskeinoja käyttämällä ei ole saatavissa riittävän oikeasuhteista, varoittavaa ja tehokasta vaikutusta. Toisaalta

---

[384] Tämä koostuu rekisterinpitäjän tietosuojaviranomaiselle ja rekisteröidylle tekemistä ilmoituksista, työntekijöiden koulutusohjelmasta, tietoturvaloukkauksista tehdyistä ilmoituksista, IT-ohjeistuksista, tietojenkäsittely- ja tietojenluovutussopimuksista kolmansien osapuolien kanssa, rekisteröityjen informoinnista (Privacy Notice), politiikoista tietoihin pääsyoikeuksiin liittyen, politiikasta liittyen rekisteröityjen mahdollisuuksiin käyttää oikeuksiaan, kuten oikeutta päästä henkilötietoihinsa ja tätä koskevasta dokumentaatiosta, lokitiedoista sekä henkilötietojen käsittelytoimintaa elinkaarimallin mukaisesti kuvaavista prosessikaavioista ja säilytysaikojen määritelmistä.

[385] Riskienhallintadokumentaatio koostuu liiketoimintaan liittyvän henkilötietojen käsittelyn riskien arvioimisesta, IT riskien arvioimisesta, uusien käsittelytoimien tietoturvallisuuden arvioimisesta (Privacy by Design) sekä tietoturvaloukkauksista ilmoittamiseen liittyvästä riskien arvioimisesta.

[386] Relevanttia dokumentaatiota ovat tällöin sekä sisäiset että ulkoiset auditointiraportit ja tietojenkäsittelysopimukset liitteineen.

[387] Adshead 2017, s. 127—133 ja 145.

tietosuoja-asetuksen 83(2) artiklan mukaan hallinnollisia sakkoja voidaan käyttää myös muiden tietosuojaviranomaisen toimivaltaan kuuluvien hallintopakkokeinojen yhteydessä niiden ohella tehosteena.

Vastuun arvioimisessa on GDPR:n 83(2) artiklan mukaan otettava huomioon rikkomuksen tai rikkomusten luonne, laajuus, vakavuus ja kesto sekä tahallisuuden tai tuottamuksen aste. Sakkoa määrättäessä on otettava huomioon rekisterinpitäjän ja henkilötietojen käsittelijän toiminta kokonaisuutena siten, että jo toteutetut tekniset ja organisatoriset toimet voivat vähentää vastuun astetta. Vastuun arvioimisessa on myös erityisestävyyteen viittaavia piirteitä, kun huomiota on kiinnitettävä myös mahdollisesti aikaisemmin määrättyihin toimenpiteisiin, jolloin näiden todettu riittämättömyys voi johtaa hallinnollisen sakon määräämiseen.

Koska koko tietosuoja-asetuksen tavoitteena on yksilön suojeleminen, tulee kiinnittää huomiota siihen, kuinka suuren riskin tai aktualisoituneen vahingon tietosuoja-asetuksen noudattamatta jättäminen aiheuttaa rekisteröidylle. Tällöin rekisteröityjen ja henkilötietojen ryhmillä sekä viimeiseksi mainittujen arkaluonteisuudella on vaikutusta tapauksen arvioinnissa. Myös yhteistyön asteella vahinkojen vähentämiseksi on merkitystä, sillä näin ollen yksilölle aiheutuva riski sekä mahdolliset vahingot voidaan saada jopa kokonaan estetyiksi tai merkittävissä määrin vähennetyiksi.[388]

# IV. OSOITUSVELVOLLISUUDEN VAIKUTUS REKISTERINPITÄJÄN TOIMINTAAN ULKOISTUSTILANTEESSA

## 1. Tekniset ja organisatoriset toimenpiteet henkilötietojen käsittelyä ulkoistettaessa

Henkilötietojen käsittelyä koskevan toiminnan arvioinnista vastuussa on rekisterinpitäjä. Rekisterinpitäjän tulee henkilötietojen käsittelyyn liittyvää toimintaa arvioidessaan huomioida myös, ulkoistetaanko käsittelytoimia henkilötietojen käsittelijöille. Tämä vaikuttaa osaltaan henkilötietojen käsittelyyn liittyvään riskiin. Henkilötietojen käsittelyn ulkoistamista on minkä tahansa käsittelytoimen siirtäminen kolmannelle osapuolelle. Näitä käsittelytoimia voivat olla esimerkiksi henkilötietojen säilyttäminen tai analysoiminen sekä jo pelkän pääsyn mahdollistaminen. Rekisterinpitäjän onkin käsittelytoimia ulkoistaessaan tunnistettava kaikki tietosuoja-asetuksen vaatimukset, joilla on merkitystä ulkoistamistilanteessa.[389]

[388] GDPR:n 83(4) ja 83(5) artiklojen perusteella hallinnollinen sakko voi olla, riippuen kumpaa säännöstä sovelletaan, enintään 10 000 000 tai 20 000 000 euroa taikka jos kyseessä on yritys niin enintään kaksi tai neljä prosenttia sen tilikauden vuotuisesta maailmanlaajuisesta kokonaisliikevaihdosta edellyttäen, että näin saatu tulo on suurempi kuin edellä mainitut yksikköarvot.

[389] Oikeusministeriön selvityksiä ja ohjeita, 4/2017, s. 22.

Olennaisinta on se, että *henkilötietojen käsittelijä*[390] kykenee myös ulkoistamistilanteessa osoittamaan ne takeet, joiden perusteella käsittelijä täyttää henkilötietojen käsittelyn edellyttämät tietosuoja-asetuksen mukaiset vaatimukset, joista säädetään käsittelijän osalta yleisen tietosuoja-asetuksen 28 artiklassa. Toisin sanoen rekisterinpitäjä ei voi ulkoistaa henkilötietojen käsittelyä sellaiselle organisaatiolle, joka ei anna riittäviä takeita rekisterinpitäjälle siitä, että tietosuoja-asetuksen vaatimukset täyttyvät. Keino näiden takeiden täyttämiselle, on solmia osapuolia *sitova oikeudellinen asiakirja*, jossa rekisterinpitäjä sitouttaa henkilötietojen käsittelijän noudattamaan hänelle tietosuoja-asetuksen nojalla kuuluvia velvoitteitaan.[391] Kyse on toisaalta myös siitä, että rekisterinpitäjä varmistaa henkilötietojen käsittelijän tunnistavan omat velvoitteensa.

Edellä mainittu oikeudellinen asiakirja, johon henkilötietojen käsittelijä tulee sitouttaa, on pääsääntöisesti toimeksiantosopimus[392]. Tietosuoja-asetuksen 28 artikla sisältää monia tarkasti määriteltyjä seikkoja, joista toimeksiantosopimuksessa on erityisesti sovittava. GDPR:n 28 artiklan tulkinnassa tulee käyttää apuna saman asetuksen johdanto-osan 81 kappaletta.[393]

Osoitusvelvollisuus edellyttää henkilötietojen käsittelyyn liittyvien prosessien sekä tietosuojakäytäntöjen toteuttamisen dokumentointia. Osoitusvelvollisuus tulee näin ollen toteuttaa pitkälti samalla tavoin kuin sisäänrakennettu ja oletusarvoinen tietosuoja, eli käytännössä rekisterinpitäjän tulee *teknisin ja organisatorisin toimenpitein* osoittaa, että tietosuoja-asetuksen asettamia velvoitteita noudatetaan. Rekisterinpitäjällä tulee olla näyttö siitä, että tämä on täytäntöönpannut tietosuojaa koskevat toimintaperiaatteet.[394]

Havainnollistavana esimerkkinä voidaan mainita tietosuoja-asetuksen 18 artikla, jonka mukaan rekisteröidyllä on oikeus siirtää henkilötietonsa yhden rekisterinpitäjän järjestelmästä toiseen jäsennellyssä, yleisesti käytetyssä sekä koneluettavassa muodossa. Kun rekisterinpitäjä on ulkoistanut henkilötietojen käsittelyn toiselle organisaatiolle, on rekisterinpitäjän tällöin edellytettävä henkilötietojen käsittelijältä sitä, että tämän järjestelmät mahdollistavat edellä kuvatun rekisteröidyn oikeuden siirtää henkilötietonsa järjestelmästä toiseen, mikäli se on teknisesti mahdollistettavissa.[395] Tämä havainnollistaa velvoitetta, jonka mukaan henkilötietojen käsittelijän tulee antaa riittävät ta-

---

Ks. myös Article 29 Data Protection Working Party, WP 236, s. 2: Tietosuojatyöryhmä on ilmoittanut antavansa tietosuojaneuvoston ohella ohjeita yleisen tietosuoja-asetuksen soveltamisesta sekä rekisterinpitäjille että henkilötietojen käsittelijöille. Tähän ohjeistukseen tutustuminen on tärkeää, jotta rekisterinpitäjän osoitusvelvollisuus sekä henkilötietojen käsittelijää koskevat vaatimukset tulevat oikealla tavalla täytetyksi.

[390] GDPR:n 4 artiklan 8-kohdan mukaan henkilötietojen käsittelijä on luonnollinen tai oikeushenkilö, viranomainen, virasto tai muu elin, joka käsittelee henkilötietoja rekisterinpitäjän lukuun.

[391] Ks. GDPR:n 28(3) artikla.

[392] Oikeusministeriön selvityksiä ja ohjeita, 4/2017, s. 22.

[393] Ks. GDPR:n johdanto-osan 81 kappale.

[394] Oikeusministeriön selvityksiä ja ohjeita, 4/2017, s. 14.

[395] Kallasvuo 2016, s. 143.

keet rekisterinpitäjälle siitä, että tämän järjestelmät on luotu sellaisiksi, joissa rekisteröityjen tietosuoja-asetuksen mukaiset oikeudet täyttyvät täysimääräisesti. Rekisterinpitäjän tulee pystyä osoittamaan, että henkilötietojen käsittelijä on sitoutettu tällaisiin velvoitteisiin ja toisaalta henkilötietojen käsittelijän tulee huolehtia, että tämän tarjoamat ohjelmistot täyttävät yleisen tietosuoja-asetuksen asettamat vaatimukset.

Tietosuoja-asetuksen 83 artiklassa määritellyt *hallinnolliset sakot* voivatkin kohdistua sekä rekisterinpitäjään että henkilötietojen käsittelijään. Mikäli ulkoistustilanteessa voidaan katsoa rekisterinpitäjän täyttävän oman osoitusvelvollisuutensa, mutta siitä huolimatta henkilötietojen käsittelijän tarjoama ohjelmisto ei täytä yleisen tietosuoja-asetuksen asettamia vaatimuksia, tulisi hallinnollisen sanktion kohdistua henkilötietojen käsittelijään eikä rekisterinpitäjään. Tällöinhän rekisterinpitäjä on hoitanut tietosuoja-asetuksen mukaisesti omat velvoitteensa.[396] On myös huomattava, että aina rekisterinpitäjä ei ole vahvempi osapuoli suhteessa henkilötietojen käsittelijään, jolla esimerkiksi ohjelmistotoimittajan ominaisuudessa voisi olettaa olevan paremmat edellytykset arvioida tarjoamiensa ohjelmistojen asianmukaisuutta.[397]

### 2. Tietojenkäsittelysopimukset

Sopimusoikeudellisena lähtökohtana pidetään sopimusvapautta, jota voidaan rajoittaa painavampien yhteisöllisten tai yksityisten etujen suojaamiseksi.[398] Henkilötietojen suojaamisen on katsottu olevan niin painava etu, että sillä voidaan rajoittaa sopimusvapautta. Tässä kohden ei ole mahdollista avata tarkemmin sopimusoikeudellista näkökulmaa, joten tuon esille ainoastaan ne seikat, jotka pakottavan tietosuojalainsäädännön nojalla tulee huomioida henkilötietojen käsittelyä ulkoistettaessa. Näissä tilanteissa osoitusvelvollisuus toteutetaan pitkälti tietojenkäsittelysopimuksilla.

Tietosuoja-asetuksen 28(3) artiklan mukaisesti henkilötietojen käsittelyä ulkoistettaessa rekisterinpitäjän tulee solmia henkilötietojen käsittelijän kanssa henkilötietojen käsittelijää sitova oikeudellinen asiakirja eli käytännössä tietojenkäsittelysopimus[399] (DPA, engl. *Data Processing Agreement*), jolla rekisterinpitäjä voi osoittaa huolehtineensa siitä, että henkilötietojen käsittelijä noudattaa unionin oikeutta sekä sovellettavaa kansallista tietosuojalainsäädäntöä. Näin ollen rekisterinpitäjällä on velvollisuus laatia tietojenkäsittelysopimus tai vastaava sitova liite muuhun sopimukseen, kun henkilötietojen käsittely tapahtuu monen eri toimijan yhteistyönä.[400] Näissä sopimuksissa ei

[396] Ks. GDPR:n johdanto-osan 82 kappale.
[397] Ks. Blume 2013, s. 140—142.
[398] Ks. esim. Schroeter 2002, s. 257—266 ja Nystén-Haarala et al. 2015, s. 99—109.
[399] DPA on aina rekisterinpitäjän ja henkilötietojen käsittelijän tai käsittelijöiden välinen sopimus. Tietojenluovutussopimus on puolestaan erillisten rekisterinpitäjien välinen sopimus.
[400] Ks. Hanninen et al. 2017, s. 82.

ole kuitenkaan kyse rekisterinpitäjien välisistä tietojen luovutussopimuksista, joita käsittelen tutkielman IV osan 3. luvussa.[401]

Komissio tai tietosuojaviranomaiset voivat julkaista vakiosopimuslausekkeita, joita voidaan käyttää yksilöllisesti laadittujen tietojenkäsittelysopimusten sijasta, mutta tällaisten vakiosopimuslausekkeiden laatiminen on ollut kuitenkin tähän mennessä varsin vähäistä.[402] Näin ollen tarkastelu keskittyy tietosuoja-asetuksen 28 artiklaan ja sen soveltamiseen.

Lähtökohtana on siis varmistaa, että henkilötietojen käsittelijä noudattaa sovellettavaa tietosuojalainsäädäntöä. Tällä tarkoitetaan tietosuoja-asetuksen 28(3) artiklan mukaan sitä, että henkilötietojen käsittelyn kohde ja kesto sekä käsittelyn luonne ja tarkoitus ovat määritelty kirjallisessa ja sitovassa muodossa. Lisäksi DPA:sta on ilmettävä, mitä henkilötietoja tullaan käsittelemään sekä mistä rekisteröityjen ryhmistä[403] käsiteltävät henkilötiedot kerätään. Myös rekisterinpitäjän tietosuojalainsäädännön mukaiset oikeudet ja velvollisuudet tulee määritellä sopimuksessa. Suurempien organisaatioiden kannattaakin laatia mallipohjia tietojenkäsittelysopimuksille, jotta tietojenkäsittelysopimuksia laadittaessa tulee aina huomioiduksi kaikki tietosuojalainsäädännöstä johtuvat relevantit velvoitteet.[404]

Tietosuoja-asetuksen 28(2) artiklan mukaan rekisterinpitäjän tulee myös vaatia, ettei henkilötietojen käsittelijä käytä muiden henkilötietojen käsittelijöiden palveluksia ilman rekisterinpitäjän ennakolta antamaa erityistä tai yleistä kirjallista ennakkolupaa. Muussa tapauksessa rekisterinpitäjä ei voisi esimerkiksi muutoksia vastustamalla riittävässä määrin huolehtia henkilötietojen käsittelijän toiminnan lainmukaisuudesta. Kuten on todettu, rekisterinpitäjän tulee voida tosiasiallisesti päättää käsittelyn tarkoituksista ja menetelmistä, vaikka käsittely suoritettaisiinkin muualla.[405]

Tietosuoja-asetuksen 28(3)(a) artiklassa edellytetään, että henkilötietojen käsittelijä suorittaa käsittelytoimet rekisterinpitäjän antaman ohjeistuksen mukaisesti. Tämä asettaa ulkoistustilanteessa rekisterinpitäjälle velvoitteen laatia kirjallinen ohjeistus henkilötietojen käsittelijälle. Käytännössä tämä tapahtuu siten, että rekisterinpitäjä antaa ohjeistuksen käsittelyn alettua ja päivittää ohjeistusta riskilähtöisesti, mikäli tämä on tarpeen. Toisaalta ei ole estettä sellaisellekaan toimintatavalle, jossa henkilötietojen käsittelijä laatii ohjeistuksen esimerkiksi palvelukuvauksessa. Edellytyksenä on kuitenkin se, että ohjeistuksen käyttökelpoisuus on riippuvainen rekisterinpitäjän hyväksynnästä.[406]

---

[401] Ks. Hanninen et al. 2017, s. 82.
[402] Ks. Ibid. s. 82—83; ks. myös GDPR:n 28(6) ja (7) artikla.
[403] Esim. rekisterinpitäjän työntekijät, asiakkaat tai potentiaaliset asiakkaat.
[404] Hanninen et al. 2017, s. 83.
[405] Article 29 Data Protection Working Party, WP 244, s. 5—6.
[406] Ks. Hanninen et al. 2017, s. 84.

Henkilötietojen käsittelyä koskevan ohjeistuksen tulee myös nimenomaisesti joko kieltää tai sallia henkilötietojen siirtämisen kolmansiin valtioihin eli EU/ETA:n ulkopuolelle.[407] Tässä yhteydessä ei voida kuitenkaan tämän syvällisemmin käsitellä näitä ohjeistuksia. Joka tapauksessa, mikäli siirto kolmansiin valtioihin sallitaan, tulisi sopimuksessa määritellä myös ne perusteet, joiden täyttyessä tällainen siirto on mahdollista. Näiden perusteiden on luonnollisesti oltava yleisen tietosuoja-asetuksen mukaisia. Tässä kohtaa tulee huomata, että tietosuoja-asetuksen 28(4) artiklan nojalla, henkilötietojen käsittelijä vastaa siitä, että tämän alihankkijat noudattavat tietosuoja-asetuksen säännöksiä, vaikka alihankkijat olisivatkin sijoittautuneet EU:n ulkopuolelle. Asetuksen kohdassa nimenomaisesti tähdennetään, että alkuperäinen henkilötietojen käsittelijä on vastuussa täysimääräisesti henkilötietojen käsittelijän velvoitteista suhteessa rekisterinpitäjään, vaikka laiminlyönti johtuisikin alihankkijan toiminnasta.

Yleisen tietosuoja-asetuksen 28(3)(b) artiklassa määrätään, että tietojenkäsittelysopimuksen tulee velvoittaa henkilötietojen käsittelijä ja tämän henkilöstö noudattamaan salassapitovelvollisuutta. Tällä tarkoitetaan sitä, että sopimuksessa tai siihen liittyvissä sitovissa asiakirjoissa on varmistettava, että tarvittaessa henkilötietoja käsittelevät työntekijät ja erityisesti mahdolliset freelancerit ja ulkopuoliset konsultit ovat sidottuja riittäviin lakisääteisiin tai sopimusperusteisiin salassapitovelvoitteisiin, mikäli heillä on pääsy henkilötietoihin.[408]

Tietosuoja-asetuksen 28(3)(c) artiklassa edellytetään, että rekisterinpitäjä, henkilötietojen käsittelyä ulkoistaessaan, nimenomaisesti velvoittaa henkilötietojen käsittelijän varmistamaan, että käsittely tapahtuu turvallisesti ja turvallisuus varmistetaan asianmukaisin toimenpitein. Tietosuoja-asetuksen 32(1) artiklan mukaan tällaisia toimenpiteitä ovat erityisesti henkilötietojen pseudonymisointi eli salanimien käyttäminen sekä kyky taata käsittelyjärjestelmien ja palveluiden jatkuva eheys, luottamuksellisuus, vikasietoisuus ja käytettävyys. Henkilötietojen käsittelijän järjestelmien tulee lisäksi olla ominaisuuksiltaan sellaisia, että on mahdollista palauttaa nopeasti tietojen saatavuus sekä pääsy tietoihin, mikäli tämä on estynyt teknisen tai fyysisen vian takia. Näiden asianmukaisten teknisten ja organisatoristen toimenpiteiden tehokkuutta tulee arvioida säännöllisesti tietojenkäsittelyn turvallisuuden varmistamiseksi. Edellä mainitut toimenpiteet liittyvät läheisesti jo aikaisemmin käsiteltyyn sisäänrakennettuun ja oletusarvoiseen tietosuojaan[409] sekä tietoturvallisuuden periaatteeseen[410].

[407] Ks. Hanninen et al. 2017, s. 85.
[408] Ks. esim. Ibid. s. 85.
[409] Ks. tutkielman III osan 4.2. luku: Sisäänrakennettu ja oletusarvoinen tietosuoja.
[410] Ks. tutkielman III osan 1.6. luku: Eheys ja luottamuksellisuus (tietoturvallisuuden periaate).

Tietosuoja-asetuksen 28(3) artiklan alakohdissa e ja f on määritelty kaksi erilaista avustamisvelvollisuutta. Alakohdan e mukaisesti henkilötietojen käsittelijä tulee sitouttaa vastaamaan rekisteröityjen tietosuoja-asetuksen mukaisiin pyyntöihin.[411] Tässä kohden on kuitenkin huomioitava käsittelyn luonne. Mikäli kyse on esimerkiksi pelkästään tietojen säilyttämisestä tai ajoittain suoritettavista järjestelmän ylläpitotoiminnoista, ei voitane pitää perusteltuna edellyttää tarkastuspyyntöihin vastaamista tai tietojen oikaisemista, vaan tällöin tämä jää täysin rekisterinpitäjän vastuulle.[412] Alakohdassa f puolestaan edellytetään, että henkilötietojen käsittelijä sitoutetaan, käsittelyn luonteesta riippumatta, avustamaan rekisterinpitäjää erikseen mainituissa rekisterinpitäjän velvoitteissa. Näitä velvoitteita ovat käsittelyn turvallisuuden varmistaminen, tietoturvaloukkauksesta ilmoittaminen tietosuojaviranomaiselle ja rekisteröidyille, vaikutusarvioinnin laatiminen sekä ennakkokuuleminen. Lienee kuitenkin perusteltua arvioida kyseisen avustamisvelvoitteen sisältöä ulkoistetun käsittelyn luonteen ja laajuuden sekä näiden pohjalta arvioitujen henkilötietojen käsittelijän tosiasiallisten mahdollisuuksien näkökulmasta, vaikka tämä velvoite onkin käsittelyn luonteesta riippumatta olemassa.[413]

Tietosuoja-asetuksen 28(3)(g) artiklassa edellytetään, että rekisterinpitäjän tulee sitouttaa henkilötietojen käsittelijä poistamaan tai palauttamaan, henkilötietojen käsittelyyn liittyvän palvelun tarjoamisen päätyttyä, kaikki henkilötiedot, ellei unionin oikeudesta tai sovellettavasta lainsäädännöstä muuta johdu. Tämä johtaa siihen, että henkilötietojen käsittelijän tulee järjestää palvelunsa siten, että kaikki tiedot ovat selkeästi palautettavissa tai poistettavissa.[414] Erityislainsäädäntö voi kuitenkin sisältää velvoitteita säilyttää tietoja vielä käsittelytoimien päättymisen jälkeenkin.[415] Esimerkiksi työsopimuslain (55/2001) 6:7.2:n mukaan työnantajalla on velvollisuus säilyttää työntekijän työtodistusta vähintään 10 vuotta työsuhteen päättymisen jälkeen. Myös kirjanpitolain (1336/1997) asettamat vaatimukset tietojen säilyttämiselle on otettava huomioon. Tässä suhteessa henkilötietojen käsittelijä joutuu säilyttämään joitakin tietoja myös rekisterinpitäjän ominaisuudessa.

Tietosuoja-asetuksen 28(3)(h) artiklan mukaan rekisterinpitäjän tulee velvoittaa henkilötietojen käsittelijä antamaan tälle kaikki tarpeelliset tiedot edellä mainittujen velvollisuuksien noudattamisen arvioimiseksi. Rekisterinpitäjällä on myös oikeus edellyttää näiden tietojen toimittamista rekiste-

[411] Ks. GDPR:n III luku (rekisteröityjen oikeudet).
[412] Ks. esim. Hanninen et al. 2017, s. 88.
[413] Ks. GDPR:n 32—36 artikla (rekisterinpitäjän velvollisuuksia).
[414] Ks. Hannila et al. 2017, s. 89.
[415] Ks. Ibid. s. 89.

rinpitäjän valtuuttamalle auditoijalle sekä määrätä henkilötietojen käsittelijä osallistumaan auditointiin.[416] Tämän velvoitteen sisältöä ei ole tarkemmin määritelty, mutta voitaneen pitää perusteltuna, ettei tällä tarkoiteta vain kertaluonteiseksi rajoitettua tietojen nähtäville saattamista.[417] Tätä velvoitetta tulisikin tulkita rekisterinpitäjän jatkuvana auditointioikeutena sen varmistamiseksi, että sovellettavaa tietosuojalainsäädäntöä noudatetaan.[418] Jotta auditointioikeuden toteuttaminen ei koituisi liian hankalaksi, olisi perusteltua edellyttää, että auditoija voi olla myös henkilötietojen käsittelijän kilpailija, mikäli palveluntarjoaja on sellaisella toimialalla, että potentiaaliset auditoijat ovat lähtökohtaisesti tämän kilpailijoita.

Kaikkien edellä mainittujen velvoitteiden tulee ilmetä tietojenkäsittelysopimuksesta tai muusta osapuolia sitovasta asiakirjasta. Tietosuoja-asetuksen 28(5) artikla ei myöskään rajoita käytännesääntöjen tai sertifiointimekanismin hyödyntämistä osatekijänä edellä mainittujen velvoitteiden täyttämisessä.[419]

### 2.1. Vahingonkorvausvastuun jakaminen

Korvausvastuuta arvioitaessa, on aina ensin selvitettävä, soveltuuko tapaukseen tietosuoja-asetus eli onko kyseessä unionin kansalaiseen kohdistunut tai unionin alueella tapahtunut henkilötietojen käsittely.[420] Muussa tapauksessa arvioitavaksi tulisivat pelkästään yleiset vahingonkorvausopit sekä kansalliset erityissäännökset, jotka rajautuvat tutkielmani ulkopuolelle.

Tietosuoja-asetus sisältää *laajan henkilötiedon määritelmän*, kuten asetusta edeltävä vuodelta 1995 peräisin oleva henkilötietodirektiivikin. Myös unionin tuomioistuin on oikeuskäytännössään vahvistanut laajan henkilötiedon määritelmän tulkinnan. Unionin tuomioistuin on todennut, että sukunimen ja etunimen[421] lisäksi myös pelkästään henkilön nimi ilmoitettuna työsuhteensa tai harrastuksiensa taikka puhelinnumeronsa kanssa[422] sekä sormenjäljet[423], IP-osoite[424] ja henkilöstä kameralla otettu kuva katsotaan henkilötiedoiksi[425]. Näiden edellä mainittujen tietojen tai näihin rinnastettavien tietojen käsittely voi johtaa rekisterinpitäjän tietosuoja-asetuksen mukaiseen vahingonkor-

[416] GDPR:n 28(3)(h) artikla.
[417] Ks. Hanninen et al. 2017, s. 89.
[418] Ks. Ibid. s. 89.
[419] Ks. Ibid. s. 106—114.
[420] Wennäkoski 2017, s. 69.
[421] EUT: Euroopan komissio v. The Bavarian Lager Co. Ltd., C-28/08 P, kohta 68 ja EUT: Colid McCullough v. Euroopan ammatillisen koulutuksen kehittämiskeskus, C-496/13, kohta 66.
[422] EUT: Rikosoikeudenkäynti v. Bodil Lindqvist, C-101/01, kohta 24.
[423] EUT: Michael Schwarz v. Stadt Bochum, C-291/12, kohta 27.
[424] EUT: Scarlet, C-70/10, kohta 51.
[425] EUT: František Ryneš v. Úřad pro ochranu osobních údajů, C-212/13, kohta 22.

vausvastuuseen. Osoitusvelvollisuudesta johtuen rekisterinpitäjän on huolehdittava, että rekisteröidyllä on yleisen tietosuoja-asetuksen mukainen mahdollisuus saada korvausta henkilötietojen käsittelyn aiheuttamasta vahingosta.

Edeltäneessä direktiivissä käytettiin ilmaisua ”*oikeus saada rekisterinpitäjältä korvausta aiheutuneista vahingoista*”, mainitsematta oikeutta täyteen korvaukseen.[426] Tietosuoja-asetuksessa lähtökohtana on sen 79 artiklan nojalla tehokkaat oikeussuojakeinot. Asetuksen 82(1) artiklassa vielä täsmennetään, että asetuksen vastaisesta toiminnasta on oikeus saada korvausta sekä rekisterinpitäjältä että henkilötietojen käsittelijältä eli kaikilta käsittelyyn osallistuneilta. Tietojenkäsittelysopimuksella tätä oikeutta ei saa rajoittaa. Asetuksen johdanto-osan 146 kappaleessa mainitaan edelleen, että rekisteröidyillä tulee olla oikeus täyteen ja tosiasialliseen korvaukseen aiheutuneista vahingoista. Vastaavaa sanamuotoa ei käytetty edeltäneessä direktiivissä.

On syytä huomata, että tietosuoja-asetuksen 2(4) artiklassa todetaan, ettei asetus rajoita direktiivin 31/2000/EY (*direktiivi sähköisestä kaupankäynnistä*) soveltamista, kun kyse on direktiivin 12—15 artikloissa säädetystä palveluntarjoajien vastuusta. Edellä mainitussa on kyse sähköisestä kaupankäynnistä ja sen mukaan palveluntarjoaja välttää vastuun, jos tämä ei ole siirron alkuunpanija tai siirron vastaanottaja taikka ei valitse eikä muuta siirrettäviä tietoja. Tätä voidaan pitää johdonmukaisena ilmentymänä *lex specialis derogat legi generali* -opista, jolloin erityislain katsotaan syrjäyttävän yleislain.[427]

Tietosuoja-asetuksen 82(1) artiklan mukaisesti täyden korvauksen periaate kattaa niin aineelliset kuin aineettomatkin vahingot. Asetuksen johdanto-osan 146 kappaleessa vielä täsmennetään, että vahinkoa tulee käsitteenä tulkita laajasti huomioiden unionin oikeuskäytäntö, ja tavalla, jossa kaikki asetuksen tavoitteet toteutuvat.

On esitetty näkemyksiä, joiden mukaan rekisterinpitäjän vastuu olisi jo edeltäneen direktiivin aikana ollut ankaraa vastuuta.[428] Tätä näkemystä ei kuitenkaan voida pitää perusteltuna, sillä kyseinen vastuu on ollut kuitenkin sellainen, josta on perinteisesti ollut mahdollista vapautua.[429] Niinpä tuottamukseen perustuvaa vastuuta voidaan pitää oikeampana tulkintana.[430]

Huomionarvoisena ja erityisesti ulkoistustilanteisiin vaikuttavana seikkana voidaan pitää sitä, että pelkkä osasyyllisyys riittää korvausvastuun muodostumiseen.[431] Nimittäin tietosuoja-asetuksen

[426] Henkilötietodirektiivin 24 artikla.
[427] Wennäkoski 2017, s. 72. Ks. myös tutkielman II osan 3.2. luku siitä, milloin lex specialis -periaate on sovellettavissa eurooppaoikeudessa.
[428] Van Alseoy 2016b, s. 69.
[429] Wennäkoski 2017, s. 75.
[430] Ibid. s. 76.
[431] Ks. Ibid. s. 76.

82(4) artiklan mukaan, jos useampi henkilötietojen käsittelijä tai rekisterinpitäjä on vastuussa käsittelystä aiheutuneesta vahingosta, on kukin heistä vastuussa koko vahingosta suhteessa vahingon kärsineeseen rekisteröityyn. Tämä johtaa siihen, että rekisteröidyllä on oikeus saada korvaus kokonaisuudessaan kärsimästään vahingosta yhdeltä vahingosta vastuussa olevalta organisaatiolta. Tällöin täyden korvauksen maksaneella organisaatiolla on oikeus tietosuoja-asetuksen johdanto-osan 146 kappaleen perusteella periä muilta käsittelyyn osallistuneilta organisaatioilta se osuus korvauksesta, joka vastaa kyseisen organisaation vastuuta aiheutuneesta vahingosta (*regressioikeus*).[432]

Suurimpia syitä sille, miksi tietojenkäsittelysopimuksia on jouduttu neuvottelemaan uudelleen tietosuoja-asetuksen siirtymäajalla, johtuu auditointioikeuden takaamisen ohella siitä, että edellä mainitusta poiketen, henkilötietojen käsittelijät ovat DPA:ssa rajoittaneet vastuutaan niin, ettei se toteudu edellä kuvatulla tavalla suhteessa rekisteröityihin. Eri asia on puolestaan se, missä määrin henkilötietojen käsittelijä on sopimusvastuussa rekisterinpitäjälle aiheutuvasta taloudellisesta vahingosta, kuten mainehaitasta, jonka osalta vastuun ylärajasta voidaan sopia. Joka tapauksessa myös henkilötietojen käsittelijän on otettava vastaan rekisteröityjen GDPR:n nojalla tekemiä vaatimuksia. Tällöin kyse on kuitenkin yksilön eikä rekisterinpitäjän suojelusta.

Osoitusvelvollisuus kytkeytyy erityisesti vahingonkorvauskysymysten osalta näyttötaakan arviointiin.[433] Kun rekisterinpitäjän vastuulla on aina osoitusvelvollisuuden täyttäminen, johtaa osoitusvelvollisuuden laiminlyöminen käytännössä siihen, että rekisterinpitäjän osuuden aiheutuneisiin vahinkoihin voidaan arvioida olevan sitä suurempaa mitä enemmän on katsottavissa rekisterinpitäjän laiminlyöneen osoitusvelvollisuuttaan.[434]

Ulkoistustilanteissa henkilötietojen käsittelijällä on vastuu vahingoista ainoastaan siltä osin, kun se ei ole kyennyt noudattamaan henkilötietojen käsittelijälle tietosuoja-asetuksessa nimenomaisesti osoitettuja yleisen tietosuoja-asetuksen mukaisia velvoitteita, joista säädetään yleisen tietosuoja-asetuksen 28 artiklassa.[435] Osoitusvelvollisuuden puitteissa rekisterinpitäjän on annettava ohjeistukset henkilötietojen käsittelijälle. Myös näiden lainmukaisten ohjeistusten vastainen toiminta, sen aiheuttaessa vahinkoa, johtaa tietosuoja-asetuksen 82(2) artiklan mukaan henkilötietojen käsittelijän korvausvastuuseen. Tämä ilmentää myös tietosuoja-asetuksen 28(10) artiklaa, jonka mukaan,

[432] Ks. myös Hanninen et al. 2017, s. 131.
[433] Ks. esim. Wennäkoski 2017, s. 80.
[434] Ks. esim. Kremer 2016, s. 139.
[435] Ks. esim. Hanninen et al. 2017, s. 130—131.

henkilötietojen käsittelijän määritellessä itse käsittelyn tarkoitukset ja keinot, tulee kyseistä henkilötietojen käsittelijää pitää rekisterinpitäjänä kyseisenlaisen käsittelyn osalta.[436] Näin ollen rekisterinpitäjän kannattaa laatia ohjeistus henkilötietojen käsittelijälle erityisen tarkasti, jotta rekisterinpitäjän vastuu ei voisi kohdentua tarpeettoman laajalti henkilötietojen käsittelijän käsittelytoimiin.

Lopuksi on syytä todeta, että tietosuoja-asetus on pakottavaa lainsäädäntöä, eikä vahingonkorvausta koskevista asetuksen säännöksistä voida edes sopimuksin poiketa siltä osin, kun vastuussa on kyse yksilön henkilötietojen suojan takaamisesta. Osoitusvelvollisuus edellyttääkin, että rekisterinpitäjä huolehtii tietojenkäsittelysopimusten olevan tietosuoja-asetuksen mukaisia, vaikka vastuu saa perustansa myös suoraan lainsäädännöstä. Korvattavaksi voi kuitenkin tulla myös sellaisia vahinkoja, joiden korvaaminen ei perustu yleiseen tietosuoja-asetukseen. Tällaisia vahinkoja ovat muun muassa rekisterinpitäjän kärsimä mainehaitta tai muut vastaavanlaiset yleensä taloudelliset vahingot. Kuten todettu, tällaisten vahinkojen korvaamisesta voi hyvinkin yksityiskohtaisesti sopia huomioimatta yleisen tietosuoja-asetuksen mukaisia vaatimuksia. Nämä vastuunrajoitukset eivät kuitenkaan vaikuta kolmansien osapuolien eli rekisteröityjen oikeuksiin, joita yleisellä tietosuoja-asetuksella turvataan.[437]

### 2.2. Henkilötietojen siirtäminen EU/ETA:n ulkopuolelle

Tietosuoja-asetuksen 40(2)(j) artiklan mukaisesti yhdistykset ja muut rekisterinpitäjiä tai henkilötietojen käsittelijöitä edustavat elimet voivat tietosuojalainsäädännön täsmentämiseksi laatia *käytännesääntöjä* kolmansiin valtioihin kohdentuvan henkilötietojen siirron toteuttamiseksi. Toimivaltainen tietosuojaviranomainen hyväksyy kyseiset käytännesäännöt, jotka tietosuojaneuvosto lopulta kokoavasti julkaisee.[438] Tällaisissa tapauksissa voidaan tietosuoja-asetuksen 42(2) artiklan nojalla hyödyntää myös edellä kuvattuja sertifiointimekanismeja[439]. Lisäksi näitä tilanteita varten voidaan laatia sellaisen yhteistä taloudellista toimintaa harjoittavan yrityksen sisälle, mikä konsernin sisäisesti siirtää henkilötietoja EU:n ja ETA:n ulkopuolelle, *yritystä koskevat sitovat säännöt* (BCR, *Binding Corporate Rules*) tietosuoja-asetuksen 47 artiklan nojalla. Toimivaltaisen tietosuojaviran-

[436] Ks. myös Article 29 Data Protection Working Party, WP 169, s. 17: Jos yhteisössä työskentelevä luonnollinen henkilö käyttää tietoja omiin tarkoituksiinsa, jotka eivät liity yrityksen toimintaan, tämä henkilö katsotaan tosiasiallisesti rekisterinpitäjäksi ja siinä ominaisuudessa vastuulliseksi; s. 22: Tietosuojan kannalta julkaisija on katsottava riippumattomaksi rekisterinpitäjäksi, jos se kerää henkilötietoja käyttäjiltä omiin tarkoituksiinsa; s. 24: Jos yhtiön internetpalvelujen tarjoaja käsittelee verkkosivuilla olevia tietoja edelleen omiin tarkoituksiinsa, on se kyseisen tietojen käsittelyn osalta rekisterinpitäjä.

[437] Hanninen et al. 2017, s. 90.

[438] GDPR:n 40(11) artikla.

[439] Esimerkkinä sertifiointimekanismista voidaan mainita tutkielman III osan 4.5. luvussa tarkemmin käsitelty ISO/IEC 27001:2017 -standardi.

omaisen tehtävänä on vahvistaa tällaiset säännöt asetuksen 63 artiklassa säädetyn yhdenmukaisuusmekanismin mukaisesti. Sääntöjen tarkoituksena on tarjota vaihtoehtoinen tiedonsiirtotapa esimerkiksi *komission hyväksymille vakiolausekkeille*, henkilötietoja siirrettäessä kolmansiin valtioihin.[440]

Tietosuoja-asetuksen tarkoituksena on turvata EU:n ja ETA:n alueella asuvien luonnollisten henkilöiden perusoikeus henkilötietojen suojaan. Globalisoituneessa Euroopassa on koettu tarpeelliseksi huolehtia tietosuojan kunnioittamisen varmistamisesta myös silloin, kun henkilötietoja siirretään tietosuoja-asetuksen 44 artiklassa tarkoitetulla tavalla kolmansiin valtioihin taikka kansainvälisille järjestöille. Kyseiset määräykset koskevat myös henkilötietojen siirtämistä kolmannesta maasta edelleen toiseen kolmanteen maahan. Kolmansiin valtioihin tapahtuvaa henkilötietojen siirtämistä koskevien asetuksen 44—50 artiklojen funktiona on varmistaa, ettei henkilötietojen siirtäminen EU:n tai ETA:n ulkopuolelle heikennä tietosuojan tasoa. Seuraavaksi käsiteltävä *Privacy Shield* -sopimus on esimerkki komission asetuksen 45 artiklan mukaisesti päättämästä järjestelystä, jonka nojalla sen soveltamisalaan kuuluvalle alueelle voidaan kyseisen järjestelyn nojalla siirtää henkilötietoja ilman komission erillistä lupaa, kunhan Privacy Shieldin mukaista menettelyä noudatetaan.

### 2.3. Privacy Shield

Marraskuussa 2013 Euroopan komissio julkaisi suosituksen *Safe Harbor* -sopimuksen parantamiseksi. Suosituksen mukaan avoimuutta olisi lisättävä tietosuojan varmistamiseksi sekä täytäntöönpanoa tehostettava ja Yhdysvaltojen viranomaisten pääsyä Safe Harborin nojalla siirrettyihin tietoihin oli rajoitettava.[441] Lähes välittömästi tämän jälkeen Yhdysvaltojen ja EU:n viranomaiset alkoivat neuvottelemaan uutta sopimusta, jonka tarkoituksena oli helpottaa henkilötietojen siirtämistä EU:n toimivallan piiristä Yhdysvaltojen viranomaisten toimivallan piiriin siten, että tietosuojan taso ei heikkenisi näissä tilanteissa. Näin syntyneen Privacy Shield -sopimuksen aikaansaamat uudet puitteet ovat merkittävästi yksityiskohtaisemmat kuin aikaisemman Safe Harborin aikakaudella.[442]

Ensinnäkin, tiedonantovelvollisuutta koskevan periaatteen mukaisesti, rekisterinpitäjän on informoitava rekisteröityjä henkilötietojen keräämisestä ja käyttötarkoituksista sekä mahdollisista kolmansista osapuolista, joille tietoja siirretään tai joille mahdollistetaan pääsy tietoihin. Safe Harborista poiketen rekisterinpitäjällä on nykyisin velvollisuus ilmoittaa rekisteröidylle myös tämän oikeuksista, ei pelkästään oikeussuojakeinoista, vaan myös muista rekisteröidyn oikeuksista, kuten oikeudesta saada pääsy omiin henkilötietoihinsa sekä saada ne oikaistuksi.[443]

---

[440] Article 29 Data Protection Working Party, WP 263, Introduction sekä kohdat 1 ja 2; Tietosuojavaltuutetun toimiston ohje: Yritystä koskevat sitovat säännöt.
[441] Weiss et al. 2016, s. 9. NSA-skandaali vaikutti olennaisesti muutostarpeen toteamiseen.
[442] Calder 2016, s. 3—7.
[443] COM(2016) 4176 final, s. 6, kohta 20; ks. myös COM(2013) 847 final, s. 6—8 Safe Harborin aikaisista velvoitteista ja niiden soveltamisesta.

Henkilötietojen eheyttä ja käyttötarkoitusten rajoittamista koskevat periaatteet pysyivät pitkälti vastaavina Safe Harboriin nähden.[444] Lisäksi tietojen luovuttamista tietoturvallisilla tekniikoilla ja prosesseilla painotetaan edelleen. Merkittävä eroavaisuus on rekisterinpitäjältä edellytettyjen toimenpiteiden kannalta se, että jokaisen kolmannen osapuolen, jolle tietoja voidaan siirtää, tulee olla sidottu sopimukseen, joka takaa riittävän tietosuojan tason.[445] Näissäkin tilanteissa on varmistettava, että rekisteröity voi edelleen vaatia tietojen poistamista, muuttamista tai oikaisemista.[446] Privacy Shieldissä on myös kiinnitetty erityistä huomiota automatisoituun päätöksentekoon, jonka osalta todetaan, että tällaisen päätöksenteon kohteeksi joutuneella on oikeus saada informaatiota päätöksen perusteena olevista erityisistä syistä ja päätöksenteon logiikasta. Näiltä osin painotetaan lisäksi tiivistä EU:n ja Yhdysvaltain viranomaisten välistä yhteistyötä.

Tietoruvallisuuden ja tehokkaan oikeuksien täytäntöönpanon sekä vastuun takaamiseksi Privacy Shield sisältää vaatimuksen, jonka mukaan yhtiöiden ja organisaatioiden on sitouduttava täysimääräisesti kaikkiin tietosuojaperiaatteisiin ja tämän varmistamiseksi on otettava käyttöön vankat tekniset ja organisatoriset mekanismit. Tämän varmistamiseksi myös Yhdysvalloissa on oltava sellainen taho, joka valvoo edellä mainittujen periaatteiden noudattamista.[447] Kaikkiin rekisteröityjen oikeuksia koskeviin yhteydenottoihin on vastattava tietyssä määräajassa, sekä eurooppalaisen *one stop shop* -periaatteen mukaisesti valitulle tietosuojaviranomaiselle on mahdollistettava osallistuminen asian käsittelyyn. Jos rekisteröityjen vaatimuksiin ei saada kohtuullista ratkaisua edellä mainittujen prosessien puitteissa Privacy Shield edellyttää yhtiöiden sitoutumista välimiesmenettelyyn osallistumiseen rekisteröidyn tekemän valituksen ratkaisemiseksi.[448]

On huomattava, että Privacy Shield soveltuu erityisesti tilanteisiin, joissa rekisterinpitäjä siirtää henkilötietoja Yhdysvaltoihin käsiteltäväksi. Näin ollen kyse on ennen kaikkea tietojenkäsittelysopimusten soveltamisalaan kuuluvista toimenpiteistä, eikä rekisterinpitäjän ja toisen rekisterinpitäjän välisten tietojenluovutussopimusten soveltamisalasta. Pääperiaatteena onkin pidetty sitä, että käsittelyn siirtyessä Yhdysvaltoihin, on tietosuojan tason pysyttävä vastaavana Euroopassa tapahtuvaan tietojen käsittelyyn nähden.[449] Tietojenkäsittelysopimuksessa on aina varmistettava, että rekisteröidyn oikeus tietosuojaan säilyy samalla tasolla kuin Privacy Shieldissä todettu vähimmäistaso, joka vastaa GDPR:n puitteissa säänneltyä tietosuojan vähimmäistasoa. Euroopassa toimivan rekisterinpitäjän näkökulmasta onkin olennaista, että henkilötietoja käsittelevä kolmas osapuoli ilmoit-

[444] COM(2016) 4176 final, s. 7, kohta 23.
[445] Ibid. s. 7, kohta 24.
[446] Ibid. s. 7, kohta 25.
[447] Ibid. s. 8, kohta 26.
[448] Ibid. s. 12, kohta 42.
[449] Ibid. s. 8—9, kohdat 28 ja 29.

taa Privacy Shieldin mukaiselle rekisterinpitäjälle, jolta tämä on vastaanottanut henkilötietoja, mikäli tietojenkäsittelyprosesseja on muutettu, jos näillä muutoksilla saattaa olla vaikutusta tietosuojan tasoon.[450]

Safe Harborin tavoin, yhdysvaltalaisten yhtiöiden on rekisteröidyttävä Privacy Shieldin noudattamiseksi, jotta näille voidaan siirtää henkilötietoja EU:n asukkaista Yhdysvaltoihin. Eroavaisuuksia on kuitenkin nykyisessä rekisteröintiprosessissa, jota hallinnoi Yhdysvalloissa virkasuhteessa toimiva tietosuojavaltuutettu. Yhdysvaltalainen yhtiö voidaan rekisteröidä kauppakomission verkkosivuilla[451] olevaan Privacy Shield -luetteloon[452], kun tämän on varmennettu toimivan Privacy Shieldissä edellytettyjen vaatimusten mukaisesti.[453]

Jos yhtiön toiminnassa on saatettu loukata yksityisyyden suojaa tai toiminnassa on havaittu muu tietosuojaan liittyvä ristiriitaisuus, unionin kansalaisilla on oikeus pyytää Yhdysvaltojen tietosuojavaltuutetulta tutkintatoimia sen varmistamiseksi, ettei Privacy Shieldin asettamia periaatteita ole rikottu. Kaikki tällaiset tutkimukset ovat julkisesti saatavilla Yhdysvaltain liittovaltion asiaa varten perustetussa rekisterissä.[454] Yhdysvaltain tietosuojavaltuutettu on liittovaltion kauppakomission virkamies, jonka tehtävien suorittaminen edellyttää tiivistä yhteistyötä EU:n sekä Yhdysvaltojen riippumattomien valvontaviranomaisten kanssa, mukaan lukien elinten, jotka valvovat Yhdysvaltojen tiedustelupalveluiden toimintaa.[455] Valitukset on käsiteltävä 45 päivän kuluessa niiden vastaanottamisesta. Unionin kansalaisilla on oikeus ottaa yhteyttä myös kansalliseen tietosuojaviranomaiseen, jonka tulee tällöin tutkia asiaa yhteistyössä FTC[456]:n kanssa.[457]

Yhdysvallat sitoutui Privacy Shieldin myötä ensimmäistä kertaa velvoitteisiin, joilla varmistetaan Euroopan komission tehokkaat valvonta- ja toimintakeinot tietosuojaperiaatteiden rikkomistilanteissa.[458] Tämän ohella Yhdysvaltain viranomaiset ovat vakuuttaneet, että unionin kansalaisiin kohdistuvassa yleiseen turvallisuuteen perustuvassa tiedustelussa sovelletaan selkeitä rajoituksia, yksityisyyden suojan takeita sekä näitä varmistavia valvontamekanismeja.[459] Lisäksi Euroopan komission on yhteistyössä Yhdysvaltojen viranomaisten kanssa laadittava Euroopan parlamentille ja neuvostolle vuosikertomus Privacy Shieldin soveltamisalaan kuuluvasta toiminnasta. Vuosikertomuk-

[450] COM(2016) 4176 final, s. 9, kohta 29.
[451] Ks. https://www.privacyshield.gov/welcome.
[452] Guide to the EU-U.S. Privacy Shield, s. 8.
[453] Privacy Shieldin liite I.
[454] Ibid.
[455] Ibid.
[456] FTC eli Federal Trade Commission on Yhdysvaltain liittovaltion kauppakomissio. Valtion virastona sen tehtävinä on vanhastaan ollut esimerkiksi kilpailu- ja kuluttajansuojaan liittyvät asiat.
[457] COM(2016) 4176 final, s. 12—13, kohta 45.
[458] Ibid. s. 35, kohta 125.
[459] Euroopan komission tiedote, 12.6.2016.

sen laadinnassa on käytettävä hyväksi sekä Yhdysvaltain että Euroopan unionin tietosuojaviranomaisia, eli myös kansalliset tietosuojaviranomaiset olisi osallistettava prosessiin.[460] Tarkastusprosessissa saatua aineistoa ei ole kuitenkaan tarkoitus julkaista kokonaisuudessaan Euroopan parlamentille ja neuvostolle, vaan näin saadusta aineistosta olisi komission toimesta laadittava yhteenveto, joka raportoidaan eteenpäin.[461]

Johtopäätöksenä voidaan todeta, että Privacy Shield takaa viiden keskeisen säännön toteutumisen henkilötietoja siirrettäessä Euroopasta Yhdysvaltoihin. Organisaation on Privacy Shieldin mukaan

- julkaistava tietojenkäsittelyä koskeva ilmoitus sisältäen yksityiskohtaiset tiedot Privacy Shieldin noudattamisestaan, tietojenkäsittelykäytännöistään, EU:n asukkaiden henkilötietojen keräämisestä, ja niiden hyödyntämisestä sekä siirtämisestä kolmansille osapuolille
- ylläpidettävä mekanismeja, joiden avulla yksilöt voivat käyttää oikeuksiaan, kuten vaatia, ettei heidän henkilötietojaan käsitellä sekä saada tarvittaessa pääsyn henkilötietoihinsa
- tehtävä sopimus kolmannen osapuolen kanssa, joka käsittelee henkilötietoja rekisterinpitäjän lukuun, ja tämän sopimuksen on oltava yhdenmukainen Privacy Shieldin asettamien vaatimusten kanssa
- tarpeellisin teknisin ja organisatorisin toimenpitein varmistettava, että henkilötietoja käsitellään ainoastaan niihin tarkoituksiin, joita varten ne on alun perin kerätty ja lisäksi varmistettava, että henkilötiedot ovat täsmällisiä ja täydellisiä sekä ajantasaisia
- tarpeellisin teknisin ja organisatorisin toimenpitein suojattava henkilötietoja katoamiselta, väärinkäytöltä, epäoikeutetulta pääsyltä, paljastumiselta, muuttumiselta ja tuhoutumiselta ottaen huomioon käsittelyyn liittyvät riskit ja henkilötietojen arkaluonteisuus.

Lisäksi julkista valtaa käyttävien on varmistettava, että yksilöllä on riittävät oikeussuojakeinot, kun tietosuojan epäillään tulleen loukatuksi. Viranomaisilla on oltava näissä tilanteissa riittävät keinot määrätä seuraamuksia Privacy Shieldin noudattamatta jättämisen johdosta ja valvoa henkilötietojen käsittelyyn osallistuvien tahojen toimintaa.

### 3. Tietojenluovutussopimukset

Henkilötietojen luovutussopimuksella tarkoitetaan kahden erillisen rekisterinpitäjän välistä sopimusta, jonka nojalla rekisterinpitäjä luovuttaa henkilötietoja toiselle rekisterinpitäjälle tämän toisen rekisterinpitäjän omia tarkoituksia varten. Tällöin tiedot vastaanottava rekisterinpitäjä määrittelee autonomisesti käsittelyn keinot tulevaisuudessa sekä vastaa osoitusvelvollisuuden täyttämisestä

[460] COM(2016) 4176 final, s. 40—41, kohdat 145—148.
[461] Ibid. s. 41, kohta 149.

oman käsittelynsä osalta.[462] Kysymyksessä voi olla myös konsernin sisäinen henkilötietojen siirtäminen konserniyhtiöltä toiselle samaan konserniin kuuluvalle yhtiölle, mikäli tapaukseen ei sovellu jäljempänä käsiteltävä yhteisrekisteriä koskeva erityissäännös.[463]

Rekisterinpitäjä voi luovuttaa henkilötietoja toiselle rekisterinpitäjälle tämän omia tarkoituksia varten ainoastaan, mikäli luovutuksensaajalla on laillinen peruste henkilötietojen käsittelemiselle. Konsernin sisällä kyse voi olla siitä, että toinen rekisterinpitäjä tulee käsittelemään henkilötietoja oikeutettuun etuun perustuen.[464] Oikeutettuun etuun perustuvassa käsittelyssä kun voi olla kyse myös toisen rekisterinpitäjän oikeutetun edun nojalla tapahtuvasta käsittelystä.[465]

Tietojenluovutussopimuksen sisällöstä ja sellaisen erillisestä laatimisvelvoitteesta ei ole säädetty tietosuoja-asetuksessa tietojenkäsittelysopimusten tapaan. Kuitenkin tällaisen sopimuksen laatimista on pidetty suositeltavana, jotta osapuolten välisistä vastuista ei myöhemmin ilmenisi epäselvyyksiä. Lisäksi tietosuoja-asetuksen mukaisen riskilähtöisyyden nojalla on olennaista, että osapuolilla on tiedossa omat vastuualueensa. Esimerkiksi GDPR:n 36(3) artiklassa todetaan, että tietosuojaviranomaisella on oikeus saada selvitys osapuolten vastuualueista. Tässä suhteessa selvityksen ei kuitenkaan tarvitse olla tietojenluovutussopimuksen mukainen sitova asiakirja, kun kyse on kahdesta erillisestä rekisterinpitäjästä, joiden välillä tietoja siirretään.

Jos luovutussopimus päädytään laatimaan, tulisi siinä täsmentää, että kyseessä on nimenomaisesti tietojenluovutussopimus eikä tietojenkäsittelysopimus. Lisäksi sopimuksen soveltamisala olisi määriteltävä siten, että ainakin sen piiriin kuuluvat tiedot, luovutushetki, luovutustapa sekä sopimuksen voimassaoloaika tulevat määritellyiksi. Myös osapuolten informointivelvoitteet olisi hyvä määritellä. Mahdollisen tietosuojaselosteen päivittämisvelvollisuuden ohella, sopimukseen olisi sisällyttävä tiedot luovuttavan yhtiön sitoumus ilmoittaa vastaanottavalle yhtiölle rekisteröityjen pyynnöstä tapahtuvista tietojen oikaisuista, käsittelyn rajoituksista ja henkilötietojen poistamisesta.[466]

### 4. Yhteisrekisterinpitäjät

Tietosuoja-asetuksen 26(1) artiklan mukaan vähintään kahden rekisterinpitäjän määritellessä käsittelyn keinot sekä tarkoituksen, on näitä pidettävä yhteisrekisterinpitäjinä. Yhteisrekisterinpitäjien tulee määritellä läpinäkyvällä tavalla vastuualueensa osoitusvelvollisuuden noudattamiseksi ja jotta voidaan varmistaa rekisteröityjen oikeuksien tehokas käyttäminen myös näissä tilanteissa, ellei yh-

[462] Hanninen et al. 2017, s. 93—94.
[463] Ibid. s. 93.
[464] Ibid. s. 95.
[465] Korpisaari et al. 2018, s. 116.
[466] Hanninen et al. 2017, s. 95—96.

teisrekisterinpitäjien vastuualueista säädetä kyseisessä tapauksessa sovellettavaksi tulevassa tietosuojalainsäädännössä erikseen. Tällaisen järjestelyn toimeenpanemiseksi rekisteröidyille voidaan nimetä yhteyspiste muun muassa informoinnin selkeyden ja yksinkertaisuuden takaamiseksi. Yhteisrekisterinpitäjien todellisten roolien sekä muiden informoinnin kannalta olennaisten tietojen on oltava tietosuoja-asetuksen 26(2) artiklan mukaisesti rekisteröityjen saatavilla. Riippumatta rekisterinpitäjien roolista ja suhteesta rekisteröityyn nähden, on yksilöllä oikeus käyttää hänelle kuuluvia oikeuksiaan kutakin rekisterinpitäjää kohtaan erikseen, vaikkei oikeuden käyttäminen olisikaan relevanttia huomioiden kyseisen yhteisrekisterinpitäjän rooli.[467]

Yhteisrekisterinpitäjyyttä koskeva säännös ilmentää myös sitä, että rekisterinpitäjyys voi syntyä kahdella eri tavalla. Ensinnäkin rekisterinpitäjän määritellessä itse käsittelyn tarkoituksen ja keinot, mutta toisaalta rekisterinpitäjyys voi muodostua myös lain nojalla. Näin ollen rekisterinpitäjän siirtäessä henkilötietoja toiselle osapuolelle, joka käsittelee tietoja lakisääteisten velvoitteidensa nojalla, on tämä toinen osapuoli itsenäinen rekisterinpitäjä[468]. Mikäli tällaisen siirron myötä ei muodostu yhteisrekisteriä, kuuluu tilanne edellä kuvatun tietojenluovutussopimuksen alaan.[469] Esimerkkinä siitä, voidaanko muodostunutta rekisteriä pitää yhteisrekisterinä, on syytä nostaa esille unionin tuomioistuimen ratkaisu František Ryneš v. Úřad pro ochranu osobních údajů, jossa rakennuksen omistanut taho teki turvallisuusalan yhtiön kanssa sopimuksen, johon perustuen kyseinen yhtiö asensi valvontakameroita rakennuksen eri osiin. Valvontakamerat asentanutta turvallisuusalan yhtiötä ei kuitenkaan voitu pitää yhteisrekisterinpitäjänä, sillä kamerat tilannut rakennuksen omistaja oli tosiasiallisesti ainut taho, joka määritteli käsittelyn tarkoitukset ja keinot.[470]

Yhteisrekisterinpitäjyydestä voi olla puolestaan kyse silloin, kun hotelliketjut, matkatoimistot sekä lentoyhtiöt perustavat yhteisen internetalustan, jonka tarkoituksena on kehittää yhteistyötä matkavarausten osalta ja kohdentaa yhteistä markkinointia asiakkaisiin. Samankaltaisia yhteisrekistereitä on esimerkiksi samaiseen allianssiin kuuluvilla lentoyhtiöillä, jolloin jatkolennot allokoidaan toiselle allianssin lentoyhtiöille. Tällöin eri toimijat päättävät yhdessä käsittelyn keskeisistä elementeistä, kuten siitä mitä tietoja kerätään, mihin tarkoituksiin ja millä keinoin sekä kuinka kauan tietoja

[467] GDPR:n 26(3) artikla.
[468] Article 29 Data Protection Working Party, WP 169, s. 19—20 ja Handbook on European Data Protection Law, 2018, s. 104—107; Esimerkiksi, jos luovutuksensaaja käsittelee henkilötietoja asianajajista annetun lain (496/1958) tai vakuutusten tarjoamisesta annetun lain (234/2018) nojalla, on kyseinen luovutuksensaaja itsenäinen rekisterinpitäjä, vaikka tämä osapuoli lakisääteisten velvoitteidensa nojalla edustaisikin henkilötiedot luovuttanutta osapuolta. Kyse on kuitenkin sellaisesta liiketoiminnasta, jonka suorittaminen on luvanvaraista. Tällöin on epätodennäköistä, että myöskään yhteisrekisterinpitäjyyttä koskeva sääntely olisi sovellettavissa.
[469] Korpisaari et al. 2018, s. 283.
[470] EUT: František Ryneš v Úřad pro ochranu osobních údajů, C-212/13, kohta 34.

käsitellään. Näissäkin tapauksissa yhteisrekisterinpitäjyys muodostuu kuitenkin ainoastaan kyseisten tietojen osalta, jolloin jokainen yksittäinen rekisterinpitäjä on yksin vastuussa esimerkiksi omien työntekijöidensä henkilötietojen käsittelystä työnantajavelvoitteidensa nojalla.[471]

Yhteisrekisterinpitäjien on erityisen tärkeää määritellä omat roolinsa muun muassa sen takia, jotta voitaisiin päätellä, kenellä osapuolella on informointivelvollisuus ja toisaalta ettei rekisteröityihin kohdenneta tarpeettoman monenkertaista, päällekkäistä ja epäselvää viestintää. Yhteisrekisterinpitäjien ei kuitenkaan tarvitse laatia keskinäistä sopimusta asiasta, sillä osapuolilla on joka tapauksessa yhteisvastuu. On myös huomattava, että tietosuoja-asetuksen johdanto-osan 62 kappaleen nojalla rekisteröityä ei tarvitse informoida sellaisista asioista, joista rekisteröidylle on jo aikaisemmin annettu tieto tai kun tietojen tallentamisesta ja luovuttamisesta nimenomaisesti säädetään laissa taikka informoiminen olisi mahdotonta tai vaatisi kohtuuttomia toimenpiteitä.

Edellä todetun mukaisesti, rekisteröity voi käyttää oikeuksiaan ketä tahansa käsittelyyn osallistuvaa tahoa, kuten rekisterinpitäjää, yhteisrekisterinpitäjää tai henkilötietojen käsittelijää kohtaan. Yhteisrekisterinpitäjyys johtaa kuitenkin siinä mielessä itsenäistä rekisterinpitäjyyttä tai DPA-tilannetta merkittävämpään yhteisvastuuseen, että jokaisella käsittelyyn osallistuvalla yhteisrekisterinpitäjällä on pakottavasta tietosuojalainsäädännöstä johtuen vastaavat velvoitteet, kuten osoitusvelvollisuus. Tämän takia ennen yhteisrekisterinpitäjäksi ryhtymistä, tulisi harkita tarkasti yhteistyökumppaneiden luotettavuutta. Toisaalta konserniyhtiöiden osalta yhteisrekisterinpitäminen ei vastaavassa määrin nosta käsittelyyn sisältyviä riskejä, kun emoyhtiö on lähtökohtaisesti saatettavissa vastuuseen muiden samaan konserniin kuuluvien yhtiöiden vastuista ja veloista. Tietosuoja-asetuksessa kun turvataan rekisteröidyn mahdollisuus saada korvaus täysimääräisesti, siltä osapuolelta, jolla on varaa suorittaa täysimääräinen korvaus[472].[473]

Esimerkiksi Yhdysvaltojen oikeuskäytännöstä löytyy ratkaisuja, joissa eurooppalainen emoyhtiö on joutunut sosiaaliseen vastuuseen tytäryhtiönsä Yhdysvalloissa aiheuttamista vahingoista, kun kyse on ihmisoikeuksiin kohdistuvasta loukkauksesta.[474] Tällainen vastuu voi olla konstruoitavissa

---

[471] Article 29 Data Protection Working Party, WP 169, s. 19: On huomattava, että kyse ei ole yhteisrekisterinpitäjyydestä puolestaan silloin, kun joku toimijoista varaa matkustajan puolesta matkat taikka hotellimajoitukset asiakkaansa lukuun. Tällöin yhteisrekisteriä ei muodostuisi, sillä käytännössä varauksen suorittanut taho ratkaisee itse käsittelyn keinot sekä kerää henkilötiedot oma-aloitteisesti.
Ks. myös Korpisaari et al. 2018, s. 283—284, todetaan samansuuntaisesti.

[472] Ks. myös Siitarinen 2004, s. 168: Sosiaalinen vastuu on yksi yhteiskuntavastuun osa-alue, jonka voidaan nähdä muodostuvan esimerkiksi monikansalliselle konsernille, perustuen tämän vahvaan asemaan yhteiskunnassa. Henkilötietojen suojaan kohdistuva loukkaus on puolestaan yksilön perus- ja ihmisoikeuksiin kohdistuva loukkaus. Sosiaalinen vastuu tarkoittaa vastuuta sidosryhmistä, esimerkiksi tytäryhtiöistä, vaikka emoyhtiö ei olisikaan käsittelyssä yhteisrekisterinpitäjänä, jolloin vastuun muodostuminen olisi käytännössä selvä asia. Sosiaalisen vastuun perusta muodostuu eettisistä arvoista, ihmisoikeuksista ja lainsäädännöstä.

[473] GDPR:n 82 artikla.

[474] USDC Southern District of New York: Ntzebesa, et al. v. Citigroup, Inc., et al. (2014) ja Superior Court of New Jersey: VW Credit, Inc. v. Coast Automotive Group, Ltd., et al. (2002) sekä Balintulo et al. v. Daimler AG et al.

myös osakeyhtiölain (OYL, 624/2006) 22:1:n ja 22:5:n mukaisen orgaanivastuun perusteella. Oikeudenmukaista olisi, että vastuu seuraisi joka tapauksessa tosiasiallisia määräyssuhteita.[475] Eurooppaoikeuden osalta huomiota voidaan kiinnittää Bryssel I-asetuksen 5(3) artiklan mukaiseen forum delicti -säännökseen, joka koskee tilannetta, jossa tytäryhtiön toiminnasta seuraa vahinkoa EU:n alueella. *Vastuun samastuksessa* on kuitenkin kyse materiaalisesta oikeudesta eikä niinkään prosessuaalisesta seikasta, jota kyseinen säännös määrittelee.

Sovellettavat materiaalisen oikeuden säännökset valitaan Rooma II -asetuksen nojalla, jolloin osakasasemaan perustuva vastuu[476] määräytyy asetuksen 1(2)(d) artiklan perusteella. Tällöin on mahdollista päätyä myös eurooppaoikeuden nojalla päätelmään, että emoyhtiö, jonka määräysvalta perustuu osake-enemmistöön, voidaan vastuun osalta samastaa tytäryhtiöön, ainakin silloin, kun lainvalintasäännösten nojalla sovellettavaksi tulee suomalainen lainsäädäntö ja oikeuskäytäntö.[477] Näin ollen on mahdollista, että emoyhtiölle konstruoidaan vastuu sellaisesta tytäryhtiönsä rekisterinpitäjänä suorittamasta henkilötietojen käsittelystä, johon emoyhtiö ei osallistu, joko vastuun samastuksen taikka sosiaalisen vastuun muodostavan ihmisoikeusloukkauksen johdosta.

## V. JOHTOPÄÄTÖS

Tutkielman perusteella voidaan todeta osoitusvelvollisuuden olevan tarpeellinen uusi tietosuojaperiaate, jonka avulla saadaan entistä tehokkaammin toteutetuksi jokaisen perusoikeustasoinen oikeus henkilötietojen suojaan. Aikaisempi oikeuskäytäntö, koskien oikeutta henkilötietojen suojaan, ilmentää myös, kuinka tarpeellisena tätä uutta tietosuojaperiaatetta voidaan pitää. Enää ei riitä, että organisaatioissa on vain julistuksenomaisia tietosuojaperiaatteita, joiden käytännön toteutuksesta ei ole mitään takeita. Jatkossa tietosuojaperiaatteiden noudattaminen tulee rekisterinpitäjän toimesta kyetä osoittamaan kaikissa henkilötietojen käsittelyn vaiheissa.

Yleinen tietosuoja-asetus muuttaa tilannetta huomattavasti oikeudenmukaisemmaksi, sillä vaikka osoitusvelvollisuus on nimenomaisesti kohdistettu rekisterinpitäjälle, sisältää tietosuoja-asetus myös henkilötietojen käsittelijään kohdistuvan pakottavan vastuun. Aikaisemmin henkilötietojen käsittelijät ovat voineet vyöryttää kaiken vastuun rekisterinpitäjälle, vaikka tosiasiassa vahingon on

(2013). Jälkimmäisessä ratkaisussa viitataan laajasti oikeuskäytäntöön, jossa eurooppalaiseen konserniin kuuluva tytäryhtiö on joutunut Yhdysvalloissa sosiaaliseen vastuuseen.

[475] Ks. myös Korkeimman oikeuden ratkaisu KKO 2001:86 vastuun kohdistamisesta tosiasiallista määräysvaltaa käyttäviin tahoihin. Toisaalta Suomesta löytyy myös vastuun samastusta koskevaa oikeuskäytäntöä (KKO 1929 II 638 ja KKO 1997:17), jossa emoyhtiön vastuu samastetaan tytäryhtiön vastuuseen. Samastus edellyttää oikeuskäytännön perusteella aina tosiasiallisen määräysvallan käyttämistä vastuun muodostumiseen johtaneessa toiminnassa.

[476] Osakasasemaan perustuvasta vastuusta säännellään Suomessa OYL 22:2:ssa.

[477] Ks. esim. Siitarinen 2004, s. 172.

aiheuttanut henkilötietojen käsittelijän toiminta, johon rekisterinpitäjä ei ole voinut mitenkään vaikuttaa. Lisäksi voidaan todeta osoitusvelvollisuudessa olevan kyse laajemmasta lainsäädäntötrendistä, jolla lisätään organisaatioiden omavalvontaa.

Tietosuoja-asetuksen soveltaminen johtaa siis siihen, että rekisterinpitäjän tulee osoitusvelvollisuuden mukaisesti tarpeellisin teknisin ja organisatorisin toimenpitein huolehtia siitä, että kaikkia tietosuojaperiaatteita noudatetaan henkilötietojen käsittelyssä. Mikäli tämän velvoitteen täyttäminen on osoitettu, ei enempää rekisterinpitäjältä voida vaatia ja tietosuojaloukkauksesta vastuulliseksi tuleekin tällöin mahdollisesti henkilötietojen käsittelijä. Tietosuoja-asetus mahdollistaakin hallinnollisten sakkojen määräämisen myös henkilötietojen käsittelijälle. Monessa tapauksessa henkilötietojen käsittelijä on paljon suurempi organisaatio ja sillä on huomattavasti paremmat keinot arvioida oman käsittelynsä ja ohjelmistojensa toiminnan lainmukaisuutta.

Konsernin näkökulmasta relevantiksi nousee erityisesti yhteisrekisterinpitäjyyttä koskeva sääntely. Tämän sääntelyn huomioonottaminen itse asiassa pohjimmiltaan yksinkertaistaa konsernin keinoja noudattaa tietosuojaperiaatteita. Tällöin konsernin ei tarvitse aina erikseen informoida rekisteröityjä, kun henkilötietoja siirretään yhteisrekisterinpitäjältä toiselle samaan konserniin kuuluvalle yhteisrekisterinpitäjälle, kunhan yhteisrekisteristä on tiedotettu asianmukaisella tavalla.

Osoitusvelvollisuuteen liittyy myös sellaisia aspekteja, joita ei tutkielman pituus huomioiden ole ollut mahdollista käsitellä laajasti tutkielmassani. Esimerkkinä voidaan mainita *selosteet* ja *tietosuojavastaavan* nimittäminen. Monikansallisessa konsernissa tilanne voi olla pulmallinen, kun periaatteessa eri valtioissa toimivat alikonsernit kuuluvat samaan konserniin pääkonsernin kanssa, mutta tosiasiassa tietosuojavastaavan funktio ei ehkä täyty, mikäli tietosuoja-asetuksen mahdollistamalla tavalla ainoastaan pääkonsernille on nimetty tietosuojavastaava.

Osoitusvelvollisuus jakautuu tutkielmani perusteella kahteen osaan. Ensinnäkin tietosuojaperiaatteita on noudatettava ja toiseksi rekisterinpitäjän tulee kyetä osoittamaan näiden periaatteiden noudattaminen. Tämä johtaakin tietotilinpäätösajatteluun, jotta osoitusvelvollisuus voisi tosiasiallisesti täyttyä. Mielestäni osoitusvelvollisuuden englanninkielinen vastine *accountability* on huomattavasti kuvaavampi ilmaisu osoitusvelvollisuudesta. Samaa termiä kun käytetään esimerkiksi kauppaoikeuden puolella ilmaisemaan kirjanpitovelvollisen vastuullisuutta muun muassa kirjanpidon oikeellisuudesta, ja osoitusvelvollisuus sisältää täysin samat elementit kuin accountability tässä yhteydessä. Henkilötietojen käsittelytoimet on siis dokumentoitava, kuten kirjanpidossa tilitapahtumat on dokumentoitava. Aika-ajoin on suoritettava sisäisiä auditointeja ja tarkastuksia, kuten kirjanpidossakin edellytetään muun muassa tilintarkastuksen muodossa tai IFRS-standardien mukaisina sisäisinä auditointeina. Toisaalta lopulta viranomaisella on oikeus tarkastaa henkilötietojen käsittelyn lainmukaisuus. Hyvin samantyyppinen toimi on esimerkiksi verotarkastus kirjanpidon puolella.

Osoitusvelvollisuus ilmenee ulkoistustilanteessa erityisesti siten, että rekisterinpitäjän on huolehdittava, että henkilötietojen käsittelijä tiedostaa omat tietosuojalainsäädännön mukaiset velvoitteensa ja antaa riittävät takeet näiden velvoitteiden toteuttamisesta. Jotta osoitusvelvollisuus tulee täytetyksi, on rekisterinpitäjän laadittava henkilötietojen käsittelijää sitova oikeudellinen asiakirja, jossa henkilötietojen käsittelijä sitoutetaan noudattamaan näitä velvoitteita ennen kuin käsittelytoimia voi aloittaa. Tietojenkäsittelysopimuksen laatimista voidaan pitää tärkeimpänä ennakollisena toimenpiteenä osoitusvelvollisuuden täyttämiseksi ulkoistustilanteissa. Myös käsittelyn aikana on suoritettava tarkastuksia ja päivitettävä tarvittaessa ohjeistuksia, jotta käsittelytoimet ovat tietosuojalainsäädännön mukaisia. On myös varauduttava siihen, että tietosuojaviranomainen tarkastaa jälkikäteen käsittelyn lainmukaisuuden. Tämä edellyttää riittävää ja selkeää dokumentaatiota sekä sitä, että rekisterinpitäjä on asianmukaisesti kartoittanut käsittelymekanismit ja niihin liittyvät riskit.

Osoitusvelvollisuudessa on kyse tietosuojaperiaatteiden noudattamisesta, ja koska periaatteet ovat optimointikäskyjä, herää kysymyksiä esimerkiksi siitä, kuinka tarkkaa dokumentaatiota lopulta edellytetään ja miten henkilötietojen käsittelijän toiminnan auditointi tulee suorittaa. Lisäksi tulee arvioida, mitä kaikkea lopulta pakottavan tietosuojalainsäädännön nojalla rekisterinpitäjä voi henkilötietojen käsittelijältä edellyttää. Yhtiöiden välillä on myös ilmennyt eriäviä näkemyksiä siitä, missä määrin henkilötietojen käsittelijä voi asettaa maksulliseksi tietosuoja-asetuksen 28 artiklassa mainittujen velvollisuuksien toteuttamisen. Voiko henkilötietojen käsittelijä esimerkiksi laskuttaa rekisterinpitäjää siitä, että henkilötietojen käsittelijä on suorittanut rekisterinpitäjän pyytämiä tietosuoja-asetuksen mukaisia tarkastustoimia tai vastannut rekisteröityjen pyyntöihin ja tehnyt näiden pohjalta korjauksia? Lähtökohtaisesti rekisteröityjen oikeuksien toteuttamisen tulee olla ilmaista rekisteröidylle. Yhteenvetona edellä mainittuun voidaan todeta, että toimijoiden on mahdollista keskinäisin sopimuksin vaikuttaa kustannusten allokoimiseen, kunhan se ei rajoita tietosuojalainsäädännön rekisteröidylle suomia oikeuksia.

Johtopäätöksenä voidaan todeta, että rekisterinpitäjältä edellytetään erilaisten keinojen käyttämistä osoitusvelvollisuutensa toteuttamiseksi tilanteissa, joissa on kyse rekisterinpitäjän sisäisestä henkilötietojen käsittelytoiminnasta verrattuna tilanteisiin, joissa on kyse rekisterinpitäjän lukuun tapahtuvasta ulkoistetusta henkilötietojen käsittelystä. Rekisterinpitäjän on laadittava monenlaista dokumentaatiota pystyäkseen osoittamaan noudattavansa tietosuojalainsäädäntöä, ja käsittelytoimintaa on auditoitava säännöllisesti tämän dokumentaation avulla tietotilinpäätösajatuksen mukaisesti.

## VI. LIITTEET

Liite 1: Osoitusvelvollisuuden täyttämisprosessi. Kaavio on tarkoitettu luettavaksi nuolien mukaisesti numerojärjestyksessä vasemmalta oikealle.